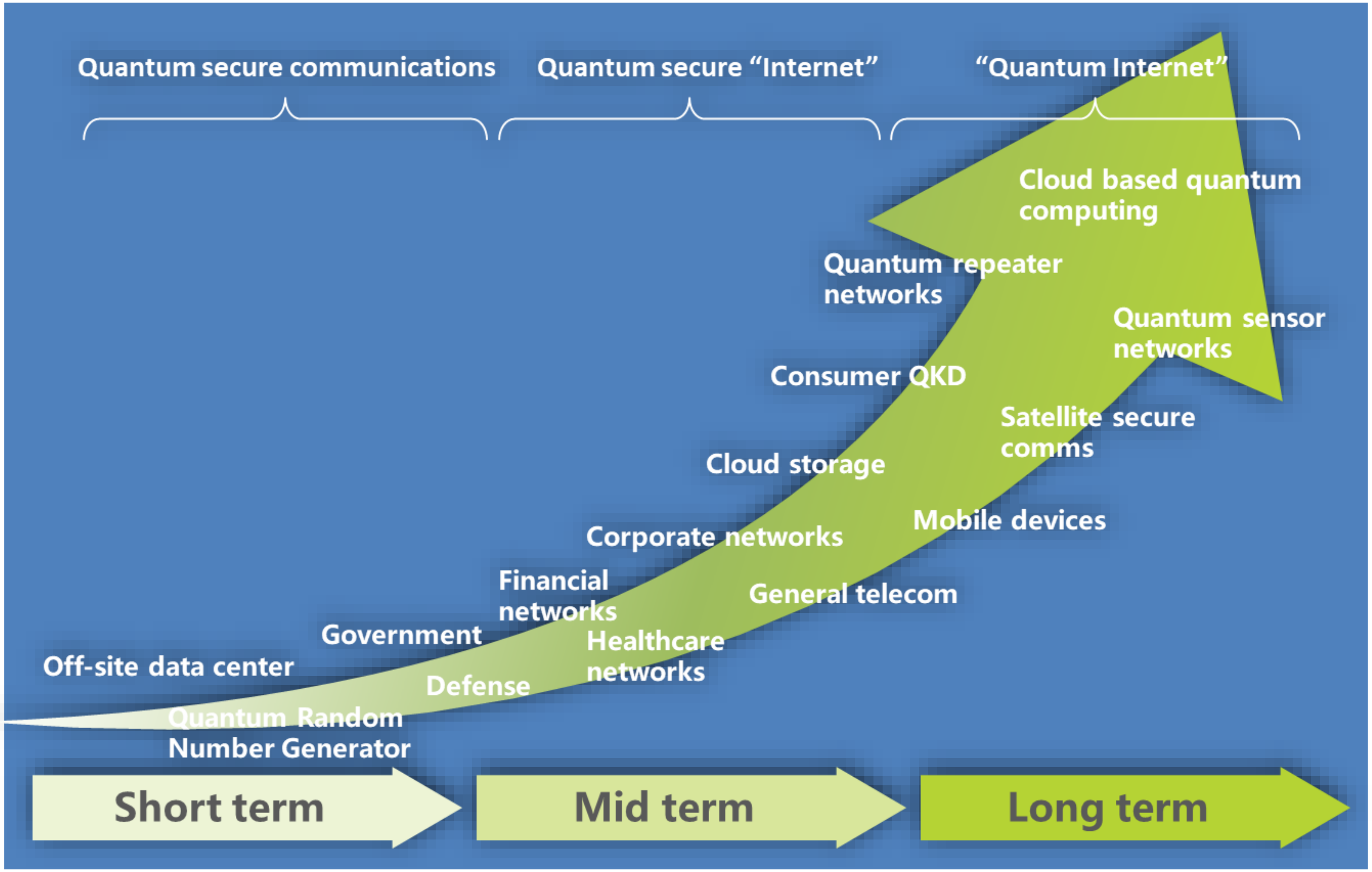
Summary of Standardization Study on Quantum Secure Communication in ITU-T FG-QIT4N and *CCSA ST7*

Zhangchao Ma
Chair of ITU-T FG-QIT4N WG2
Vice chair of CCSA-ST7 WG2

Evolution of Quantum-based Networks



The future QIN is expected to connect various quantum information processing nodes, including QKD nodes, quantum computers and quantum sensors, to realize quantum information transmission and networking.

Ref: "The Quantum Age: technological opportunities", the Government Office for Science, UK (2016)

FG-QIT4N Work Chart

Co-Chairmen

- Mr. Alexey Borodin, Rostelecom, Russian Federation
- Mr. James Nagel, L3Harris Technologies, USA
- Mr. Qiang Zhang, University of Science and Technology of China (USTC), China

Working Group Chairs

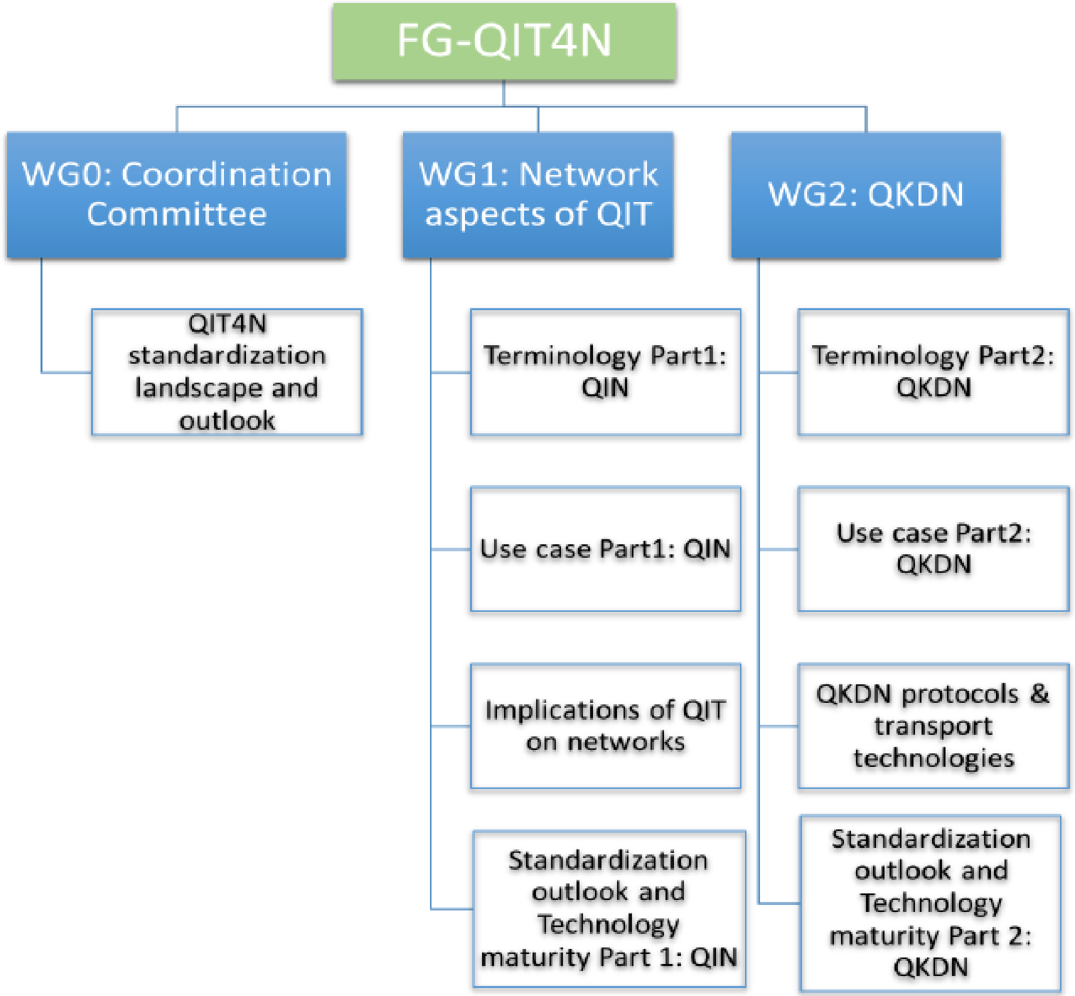
- WG0: Co-Chairmen
- WG1: Mr. Helmut Griesser, Adva Optical Networking, Germany
- WG2: Mr. Zhangchao Ma, CAS Quantum Network, China

WG1: Network aspects of QIT

To provide technical context in relation to the study topics and deliverables related to network aspects of quantum information technology

WG2: QKDN

To provide technical context in relation to the study topics and deliverables related to quantum key distribution networks and those aspects not covered in SG 13 and SG 17


FG-QIT4N

WG0: Coordination Committee

QIT4N standardization landscape and outlook

WG1: Network aspects of QIT

Terminology Part1: QIN

Use case Part1: QIN

Implications of QIT on networks

Standardization outlook and Technology maturity Part 1: QIN

WG2: QKDN

Terminology Part2: QKDN

Use case Part2: QKDN

QKDN protocols & transport technologies

Standardization outlook and Technology maturity Part 2: QKDN

Adopted at the first meeting of the FG-QIT4N, Jinan, China, December 2019

https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx

FG-QIT4N Deliverables (WG1)

Deliverables (Number, link, title)		Description
D1.1	QIT4N terminology part 1: Network aspects of QIT	A survey of terminology relevant to the network aspects of quantum information technology for networks (beyond QKDN) that supports the building blocks for QINs, application-driven network requirements, the benefits to classical networks and that will support the deliverables of FG-QIT4N WG1.
D1.2	QIT4N use case part 1: Network aspects of QIT	Study the various use cases of quantum information technologies for networks (beyond QKDN) describing use cases based on QIN, use cases beneficial to classical networks and use cases where the network plays an intrinsic role for the QIT applications.
D1.4	QIT4N standardization outlook and technology maturity part 1: Network aspects of QIT	Provides a snapshot of the standardization landscape of QIT for networks, prospects and barriers to the development and adoption of standards for QIT for networks and a review of methodologies for assessing technology maturity and standardization readiness of QIT for networks.

Way Forward:

- SG13 Q16 is actively studying the standardization aspects of QIN:
  - QIN use cases in **TR-QN-UC "Use cases of quantum networks beyond QKDN"**
  - Y.Sup75 "Quantum-Enabled Future Networks" finished and further proposing to standardize **the overview/framework of Quantum Networks**

FG-QIT4N Deliverables (WG2)

Deliverables (Number, link, title)		Description
D2.1	QIT4N terminology part 2: quantum key distribution network	Survey on existing terminology lists relevant to QKDN that exist or are in preparatory phases, with identification of any gaps or opportunities that other efforts may have been overlooked.
D2.2	QIT4N use case part 2: quantum key distribution network	Study use cases of quantum key distribution networks highlighting the competitive advantage of use cases brought by QKDN, the main barriers to QKDN adoption, and the benefits and needs for future standardization efforts.
D2.3.1	QKDN protocols part I: Quantum layer	Study and review protocols in the quantum layer of the quantum key distribution network including different types of QKD protocols, their workflows, protocol features, parameters, commercialization status, security proofs, potential to be integrated in the future network etc. and discussions & suggestions on future plans.
D2.3.2	QKDN protocols part II: Key management, QKDN control layer and management layer	Study communication protocols related to key management layer, QKDN control layer, and QKDN management layer in the QKDN. In particular, the scope of this draft technical report includes Protocols with respect to key management layer, protocols with respect to QKDN control layer, protocols with respect to QKDN management layer and provides suggestions for future works.
D2.4	QKDN transport technologies	Study QKDN transport technologies such as transport system components, technical solutions, requirements for co-fibre transmission of quantum and classical signals, etc.
D2.5	QIT4N standardization outlook and technology maturity part 2: quantum key distribution network	Study standardization outlook and technology maturity of quantum key distribution networks (QKDN), including an overview of QKDN technologies and industry development, assessment of QKDN technologies maturity, QKDN standardization landscape and gap analysis and an outlook of QKDN standardization.

FG-QIT4N Deliverables (WG2)

Deliverables (Number, link, title)	
D2.1	QIT4N terminology part 2: quantum key distribution network
D2.2	QIT4N use case part 2: quantum key distribution network
D2.3.1	QKDN protocols part I: Quantum layer
D2.3.2	QKDN protocols part II: Key management, QKDN control layer and management layer
D2.4	QKDN transport technologies
D2.5	QIT4N standardization outlook and technology maturity part 2: quantum key distribution network

Way Forward:

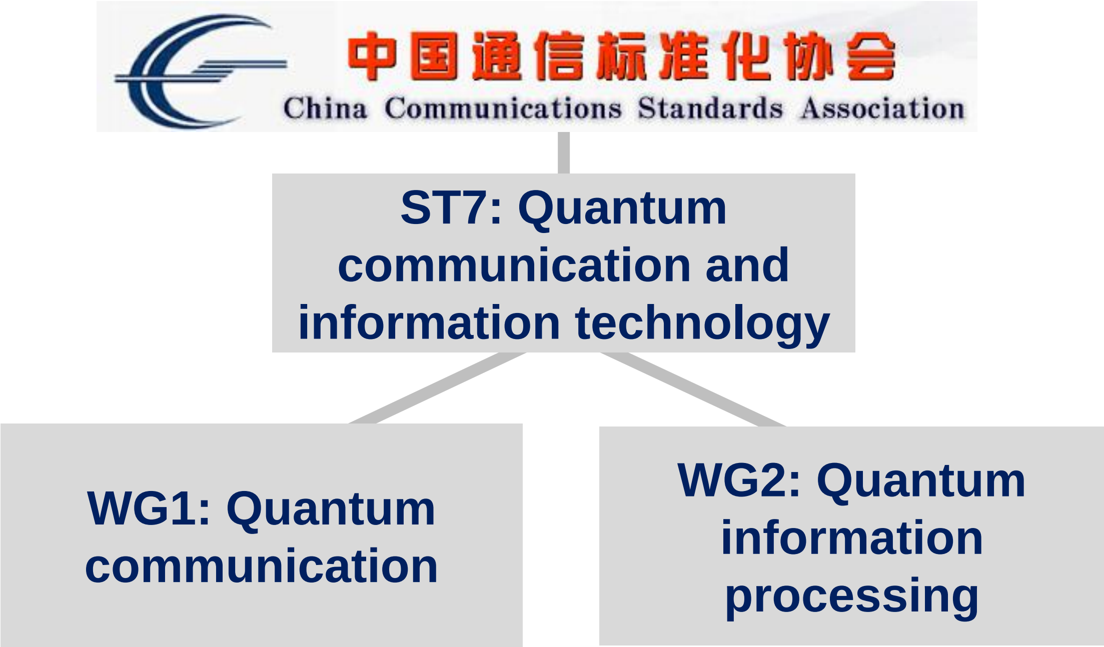
- **D2.2:** SG13 Q16 is further studying the standardization aspects of QKDN use cases in **Y.supp.QKDN-UC,** new use cases being standarding, e.g., QKDN integrating with SSN in **Y.QKDN_SSNx,** QKDN integrating with TSN in **Y.QKDN-TSNx**
- **D2.3.1:** SG17 Q15 is standardization the quantum layer QKD protocols in **X.sec_QKD_profr**
- **D2.3.2:** SG11 Q2 is actively standardizing a series of QKDN high layer protocols in **Q.QKDN_Ak/Ck/Kq/Kx …**

Introduction of CCSA ST7

- **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**



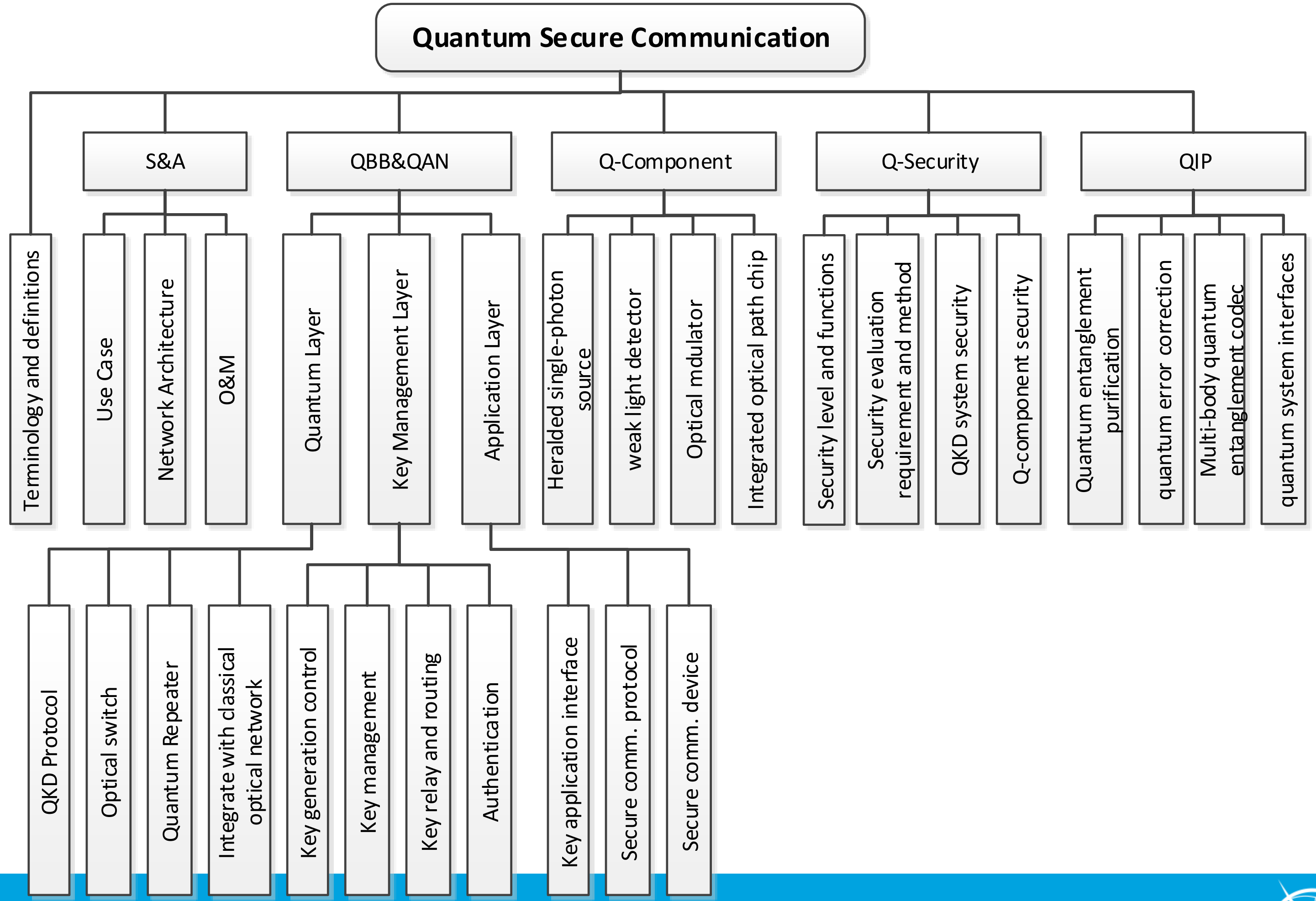
ST7: Quantum communication and information technology

WG1: Quantum communication

WG2: Quantum information processing

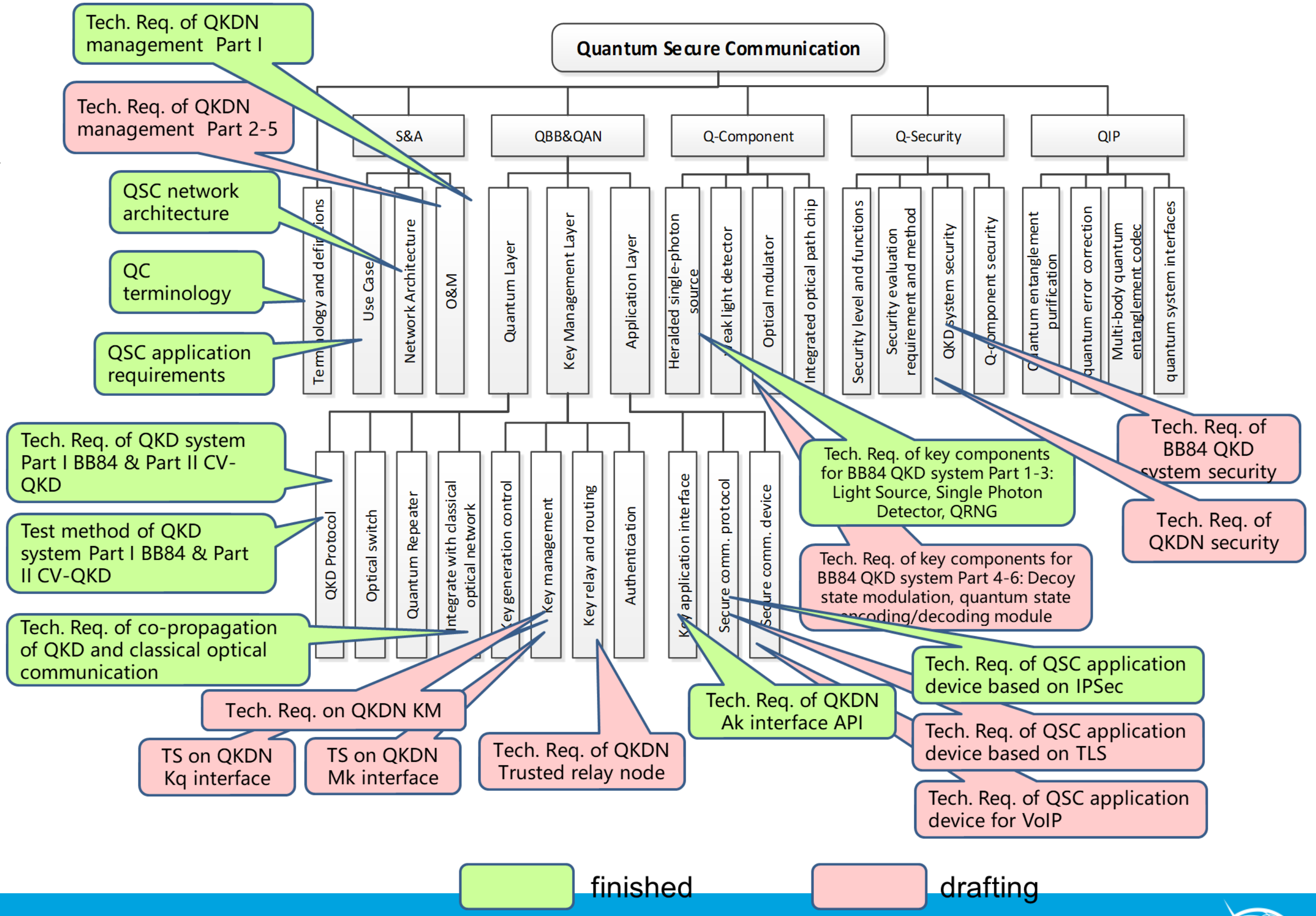
Standardization framework on QSC in CCSA

- Standards grouped into 5 classes:
  - **Service and Architecture**
  - **Backbone and access networks**
  - **Key Components**
  - **Security Requirements**
  - **Quantum Information processing**



Standardization progress on QSC in CCSA

- **14 standards finished:** QSC application requirements, QC terminology, BB84-based and GMCS-based QKD system tech. req. and test methods, QKD key components including QRNG, quantum light source, single photon detector, QKDN arch, QKDN management Part I, IPSec VPN, Ak API, Co-propagation, etc.
- **18 reports finished:** network architecture, security, trusted relay, test method, network management, decoy state protocol, co-propagation, QRNG, CV-QKD, SDN control, networking tech., space quantum communication, quantum integrated chips, TF-QKD protocol, etc.
- **15 WIs and 12 Sis ongoing**



Quantum Secure Communication

S&A: Terminology and definitions; Use Case; Network Architecture; O&M

QBB&QAN: Quantum Layer; Key Management Layer; Application Layer

Quantum Layer: QKD Protocol; Optical switch; Quantum Repeater; Integrate with classical optical network

Key Management Layer: Key generation control; Key management; Key relay and routing; Authentication

Application Layer: Key application interface; Secure comm. protocol; Secure comm. device

Q-Component: Heralded single-photon source; Weak light detector; Optical mdulator; Integrated optical path chip

Q-Security: Security level and functions; Security evaluation requirement and method; QKD system security; Q-component security

QIP: Quantum entanglement purification; quantum error correction; Multi-body quantum entanglement codec; quantum system interfaces

Tech. Req. of QKDN management Part I

Tech. Req. of QKDN management Part 2-5

QSC network architecture

QC terminology

QSC application requirements

Tech. Req. of QKD system Part I BB84 & Part II CV-QKD

Test method of QKD system Part I BB84 & Part II CV-QKD

Tech. Req. of co-propagation of QKD and classical optical communication

Tech. Req. on QKDN KM

TS on QKDN Kq interface

TS on QKDN Mk interface

Tech. Req. of QKDN Trusted relay node

Tech. Req. of QKDN Ak interface API

Tech. Req. of key components for BB84 QKD system Part 1-3: Light Source, Single Photon Detector, QRNG

Tech. Req. of key components for BB84 QKD system Part 4-6: Decoy state modulation, quantum state encoding/decoding module

Tech. Req. of BB84 QKD system security

Tech. Req. of QKDN security

Tech. Req. of QSC application device based on IPSec

Tech. Req. of QSC application device based on TLS

Tech. Req. of QSC application device for VoIP

🟩 finished 🟥 drafting

Summary and Suggestions

- Continue to promote knowledge sharing and cooperation **among SDOs** to resolve the key issues for quantum network standardization:
  - **Promote Application:** to flourish QKDN-based services
  - **Ensure Inter-operability:** to ensure quantum network interworking capability
  - **Facilitate Security certification:** to provide measurable security guarantee for QKDN
  - **Enable future evolution:** to pave the way towards future quantum network step by step

Thank you!