ETSI ISG QKD/ITU-T FG-QIT4N
Joint session
June 10, 2020
E-meeting

Quantum key distribution network protocols and transport technologies in FG-QIT4N

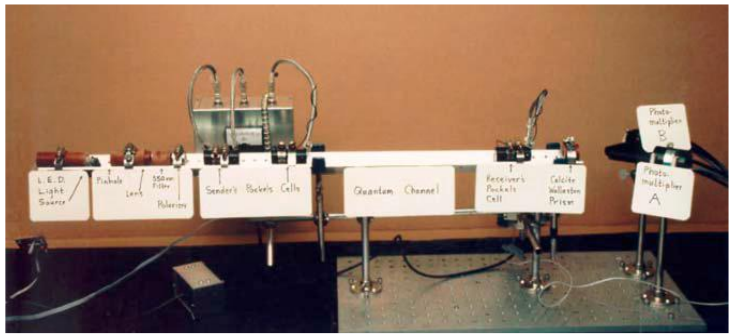
Hao Qin*#
CAS Quantum Network Co., Ltd.

Collaboration with
Hongyu Wu (WG 2 D2.3), Yalin Li (WG 2 D2.4), QuantumCTek
Peng Huang (WG 2 D2.3) , XT Quantech

#qinhao@casquantumnet.com

Quantum key distribution: From concept to applications

- Quantum key distribution (QKD)
- Information theoretic secuity based on quantum physics



- First QKD experiment in IBM 1992

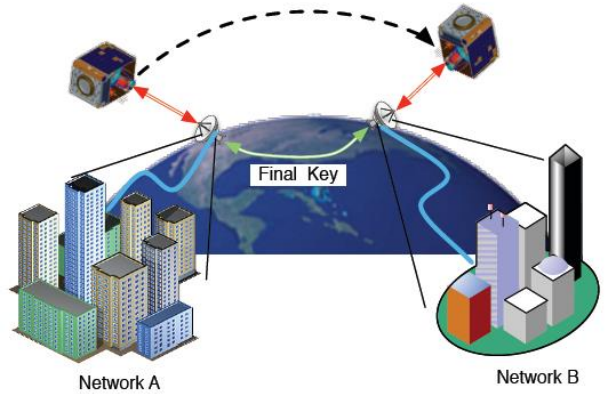
QKD satellite

ID Quantique Cerberis3 QKD

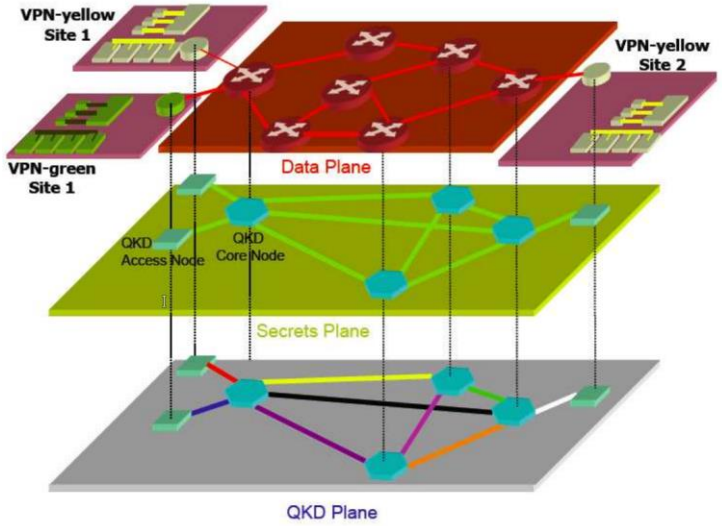
QuantumCTek SJJ1411 QKD

Toshiba GHz QKD prototype

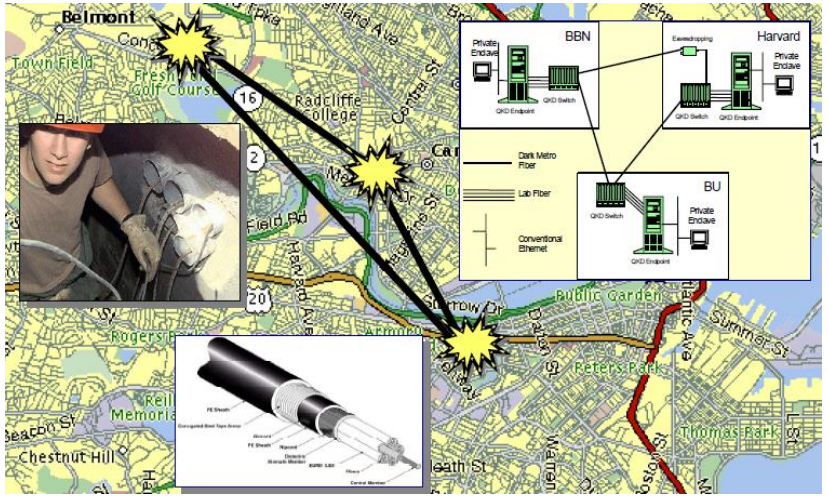
XT Quantech QDM500S



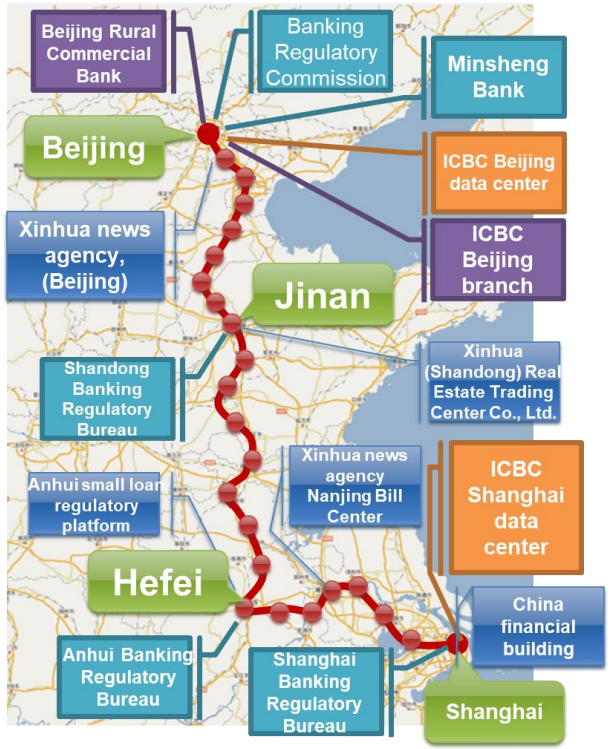
QKD networks (QKDN) based on trusted nodes around the world



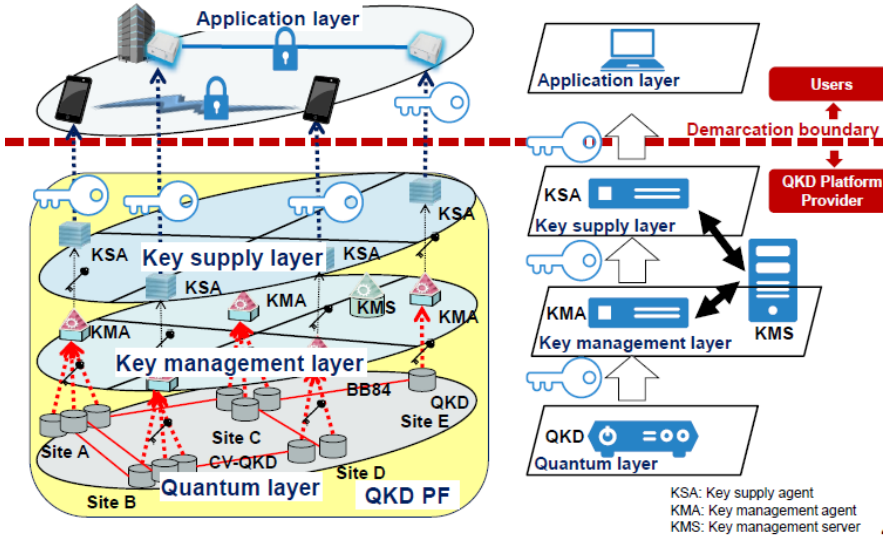
EU SECOQC QKD network, 10.1002/sec.13 (2008)



DARPA QUANTUM NETWORK，BBN Technology (2007)



QKD applications along Beijing-Shanghai Quantum Backbone (2017)



Tokyo QKD network, OE.19.010387 (2011)

SwissQuantum QKD network, NJP **13**(12), 123001 (2011)

AND SO ON……

Pre-standardization and technical reports

- **Technical Reports**
  - No normative contents
  - Contents based on contribuations
  - Standardization studies and analysis
  - References and suggestions for further standardizations in SDOs

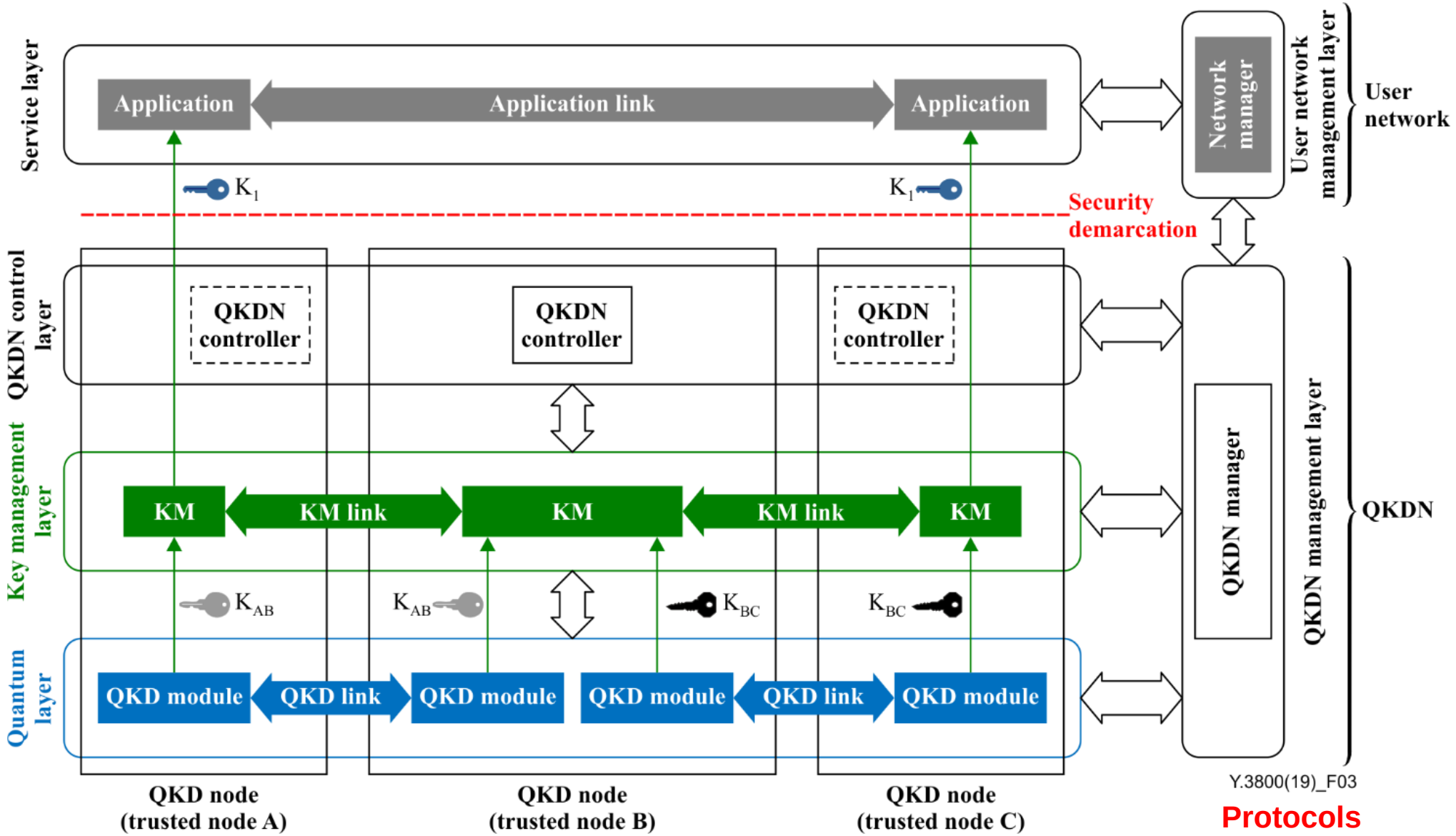
- **WG 2 D2.3: QKDN protocols**
  - Part 1: Quantum layer
  - Part 2: Classical layers

- **WG 2 D2.4: QKDN transport technologies**
  - QKD system implementation technolgies
  - Co-existing with classical signals

Structure of QKDN based on trusted nodes

- Protocols Part 2

- Protocols Part 1
- Transport technologies

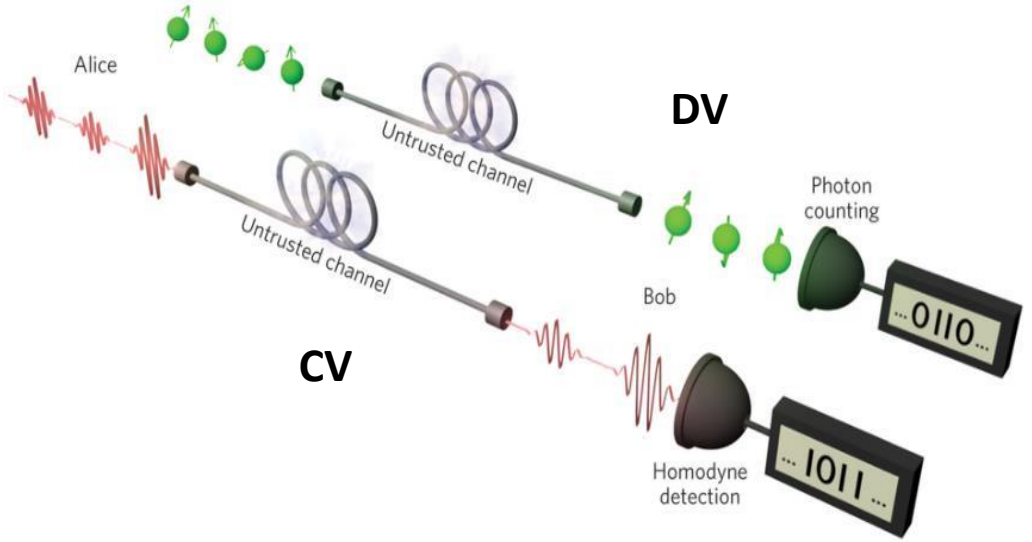


Conceptual structures of a QKDN and a user network in Rec. ITU-T Y.3800 (10/2019)

Protocols Part 2

QKDN protocols Part 1: Quantum layer

- **Scope**
  - Introduction of QKD protocols:
    Discrete variable & Continuous variable
  - Workflows, features, parameters
  - Commercialization, security proofs status
  - Discussions & suggestions on future works
- From the perspective of standardizations, for tne readers in SDOs



Nature Photonics 7,350–352 (2013)

QKDN protocols Part 1: Quantum layer

NIST plans to release draft standards for PQC algorithms in 2022, will any QKD protocol standards be there by that time?

- Many review papers on QKD protocol already there, why another report?
- QKD protocols only appear in research papers, none of them are standardized for over 30 years.
  - Debates on QKD protocol standardizations
- In classical cryptography and post quantum cryptography, protocol standardization is the first priority.
  - An essential step for system evaluation and certification
  - Missing standards is a roadblock for wider use of QKD

QKDN protocols Part 1: Quantum layer

- Work plan

- Introduce QKD protocols under the umbrella of FG-QIT4N

- Mainly for readers with no QKD backgrounds but works on standards in SDOs
  - Briefly introduce improtant aspects of QKD protocols
  - Analysis and discussions on whether QKD protocol standardization is necessary: **Pros** and **Cons**
  - Try to reflect different points of views and give suggestions on further works

- Contributions from various sources are welcome

QKDN protocols Part 2: Classical layers

- **Scope**
  - Identify and study protocols in classical layers: key management layer, QKDN control layer, QKDN management layer
  - Give some examples of protocol workflow, operation, parameters.
  - Identify gap and standardization analysis
  - Suggestions for future works

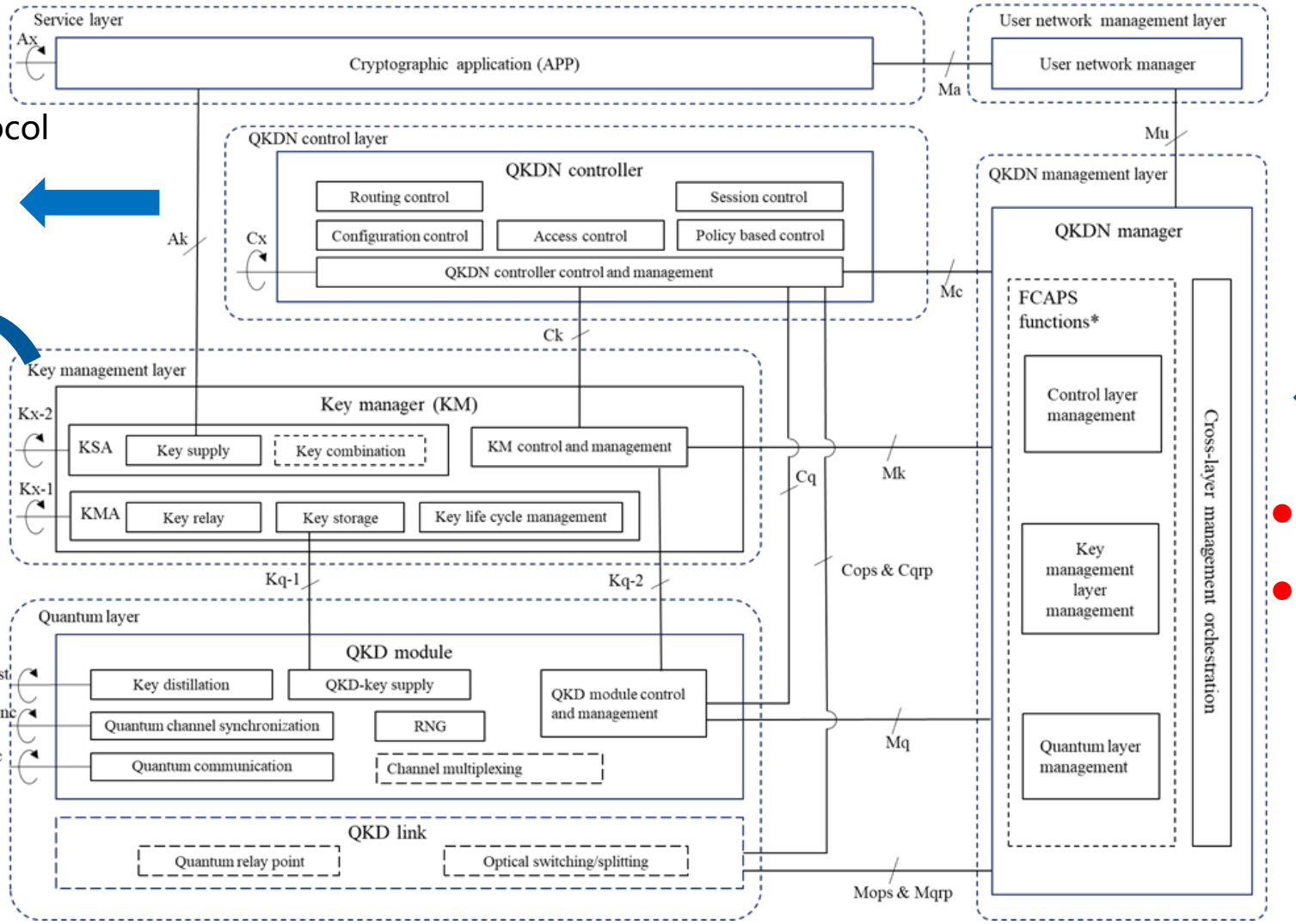
    Unified interfaces and protocols will help different vendors provide compatible equipment or systems.

QKDN protocols Part 2: Classical layers

- Functional architecture model of QKDN and underlying protocols

- Key generation control protocol
- Routing control protocol
- Session control protocol
- Access control protocol
- QoS control protocol

- Key acquisition protocol
- Key relay protocol
- Key supply protocol



- FCAPS management protocols
- Cross-layer orchestration protocols

Draft Recommendation ITU-T Y.QKDN_Arch under development in SG 13

QKDN protocols Part 2: Classical layers

- Protocol operations and message parameters

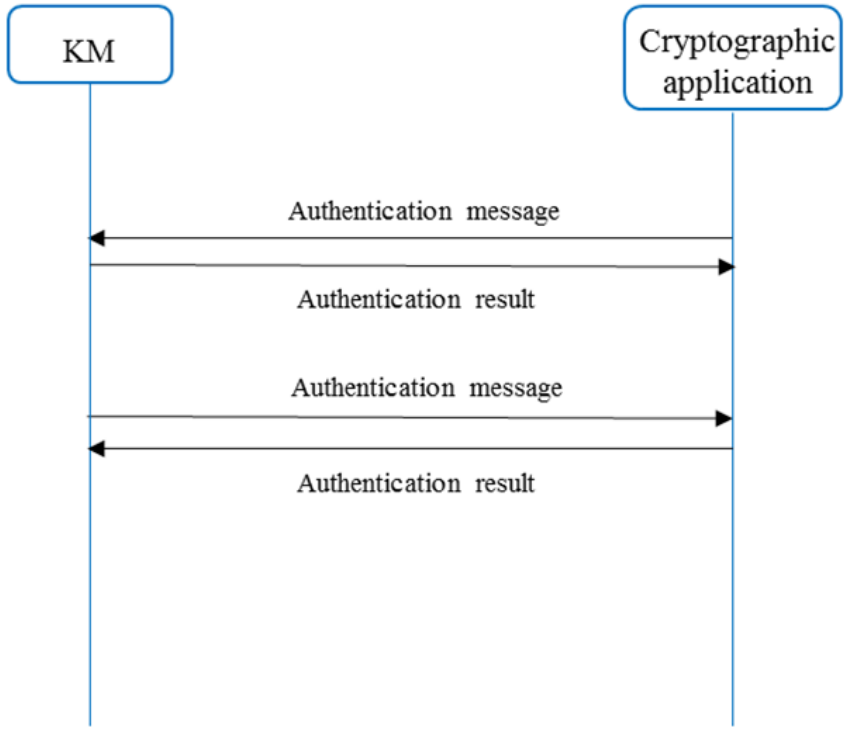


Table 7.x.1 Command message for authentication

Item	Description	Remark
Message ID	A message identifier generated by a sender of the command message for authentication.	
Command Code	A code that indicates the command message is used for authentication.	
Sender ID	Unique ID of the sender of the command message for authentication.	
Authentication Info	Information used for authentication.	The authentication information is configurable and may be generated by algorithms.
……		

Table 7.x.2 Response message for authentication

Item	Description	Remark
Message ID	A message identifier generated by a sender of the response message for authentication.	
OrigMessage ID	A message identifier received from a command message for authentication.	
Command Code	A code that indicates the response message is used for authentication.	
Sender ID	Unique ID of the sender of the response message for authentication.	
Response Code	A code that indicates an authentication result.	0x01: success 0x02: failure
……		

- Protocols with at least protocol operations and message parameters are invited.
- Experts on protocols or security issues are welcome to contribute on this report.

QKDN transport technologies

- **Scope**

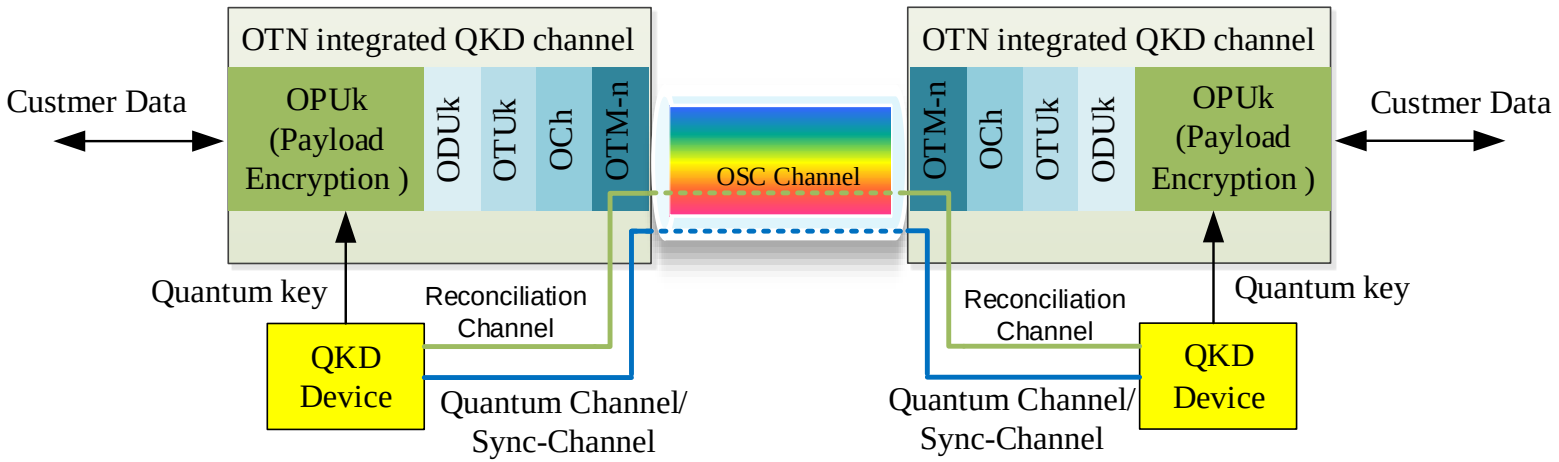
  The report includes studies of QKDN transport technologies

  - Transport system components of QKDN
  - Transport technology solutions for QKDN
  - Technical requirements for co-fiber transmission of quantum and classical signals, etc.
  - Suggestions for future works

  The studies are organized with two parts: DV-QKD and CV-QKD.

QKDN transport technologies

- **Work completed**
  - General introduction of CV-QKD systems, as part of the QKD system introduction
  - Co-fiber transmission schemes of QKD with classic optical communication systems
    - one example of the schemes is shown below
    - some experimental studies and noise analysis

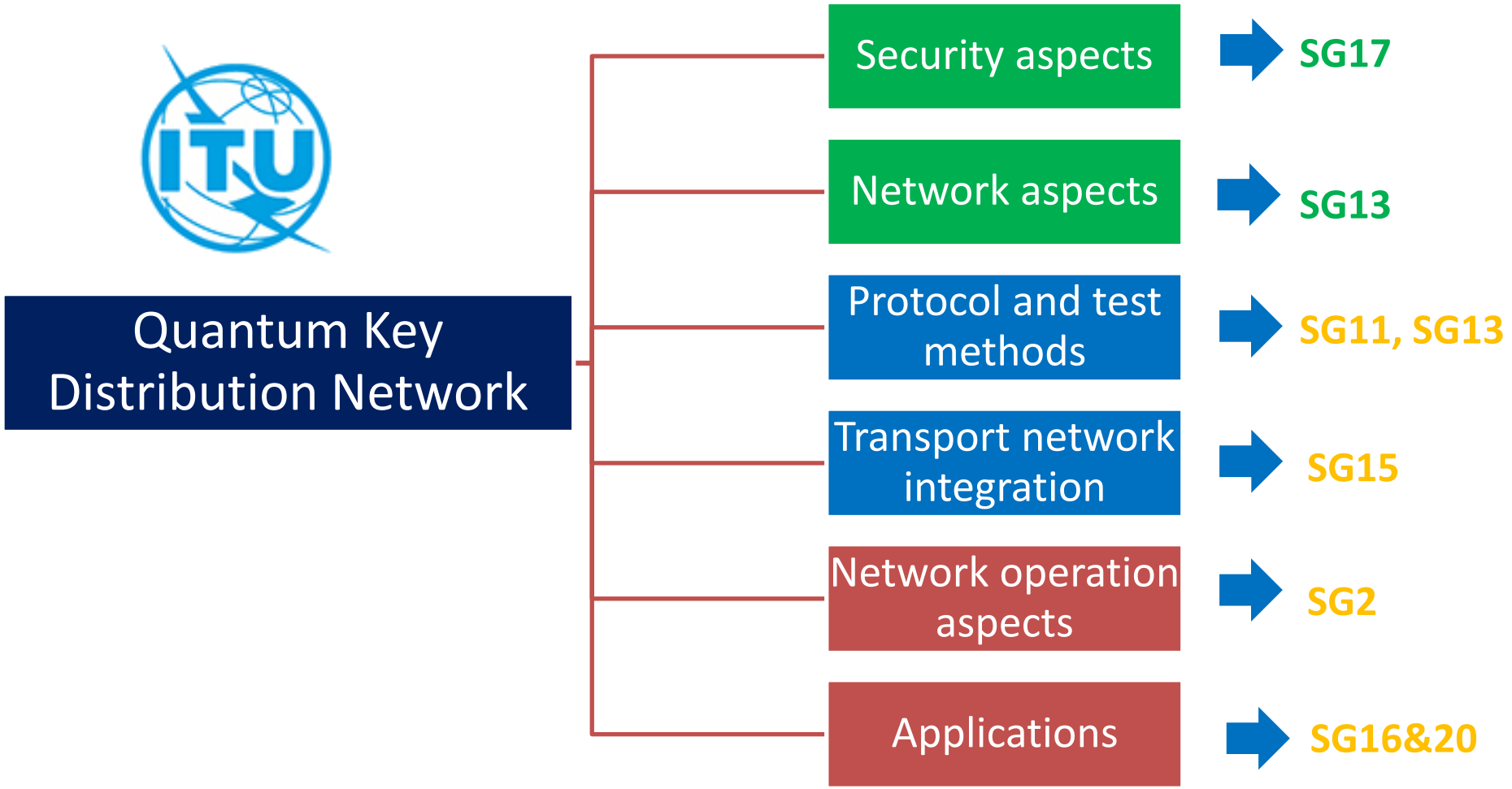


QKDN transport technologies

- **Next work**
  - An overview of QKDN transport technologies
  - Some experimental results based on the co-fiber schemes as examples
  - Suggestions for QKDN with co-fiber technologies
  - New research results and suggestions from experts are highly appreciated

What is next?

Current works in FG-QIT4N D2.3, D2.4
Ongoing studies in ITU-T study groups
Potential studies after FG-QIT4N



ISO

ETSI
World Class Standards


Thanks.