QCrypt 2020
Industry session
August 12, 2020
E-meeting

Standardization of quantum cryptography in ITU-T and ISO/IEC

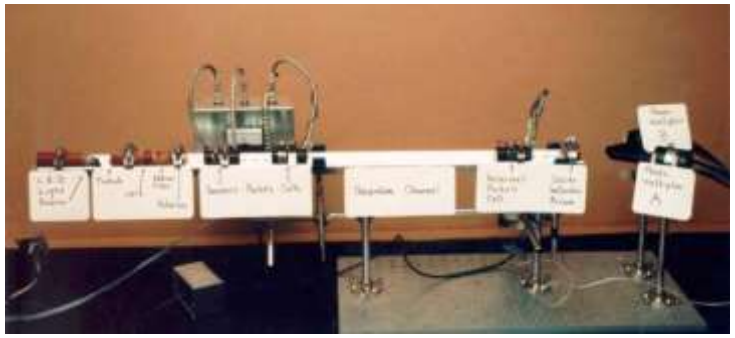
Hao Qin*

CAS Quantum Network Co., Ltd.

*qinhao@casquantumnet.com

Quantum key distribution: From concepts to applications

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



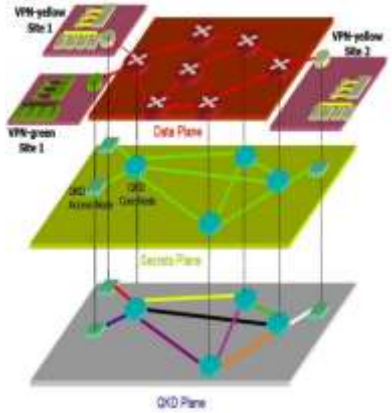
- First QKD experiment in IBM 1992

QKD satellite

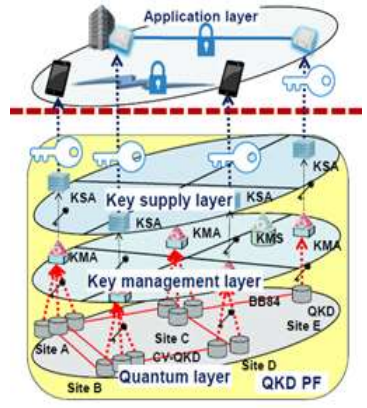
QKD commercial products

IDQ, QCTEK, Toshiba, QRate, XT etc.

QKD Network (QKDN)



EU SECOQC



Tokyo Network

Beijing-Shanghai Backbone

International Standards Development Organizations (SDOs)

International Organization for Standardization (ISO)

- Non-Governmental Organization, founded in **1947**
- An international standard-setting body composed of representatives from various national standards organizations
- Promotes worldwide proprietary, industrial, and commercial standards

International Electro-technical Commission (IEC)

- Not-for-profit, quasi-governmental organization, founded in **1906**
- International standards for all electrical, electronic and related technologies, known as "electrotechnology".

International Telecommunication Union (ITU)

- Originally the International Telegraph Union created in **1865**
- A specialized agency of the United Nations for information and communication technologies
- The oldest global international organization
- The first international standards organization

Standardization activities in SDOs

- European Telecommunications Standards Institute (**ETSI**)
  - Standardization activities of QKD since 2008
  - All aspects of QKD: 8 specifications, 2 white papers

- **ISO/IEC JTC1**
  - Information technology
    - SC 27 WG 3: QKD implementation security
    - SC 27 WG 2: Post quantum cryptography (PQC)
    - WG 14: Quantum computing

- International Telecommunication Union (**ITU**)
  - SG 13: QKDN network aspects
  - SG 17: QKDN security aspects
  - FG QIT4N WG2: QKDN terminology, use cases, protocols, transport etc (Pre-standardization)

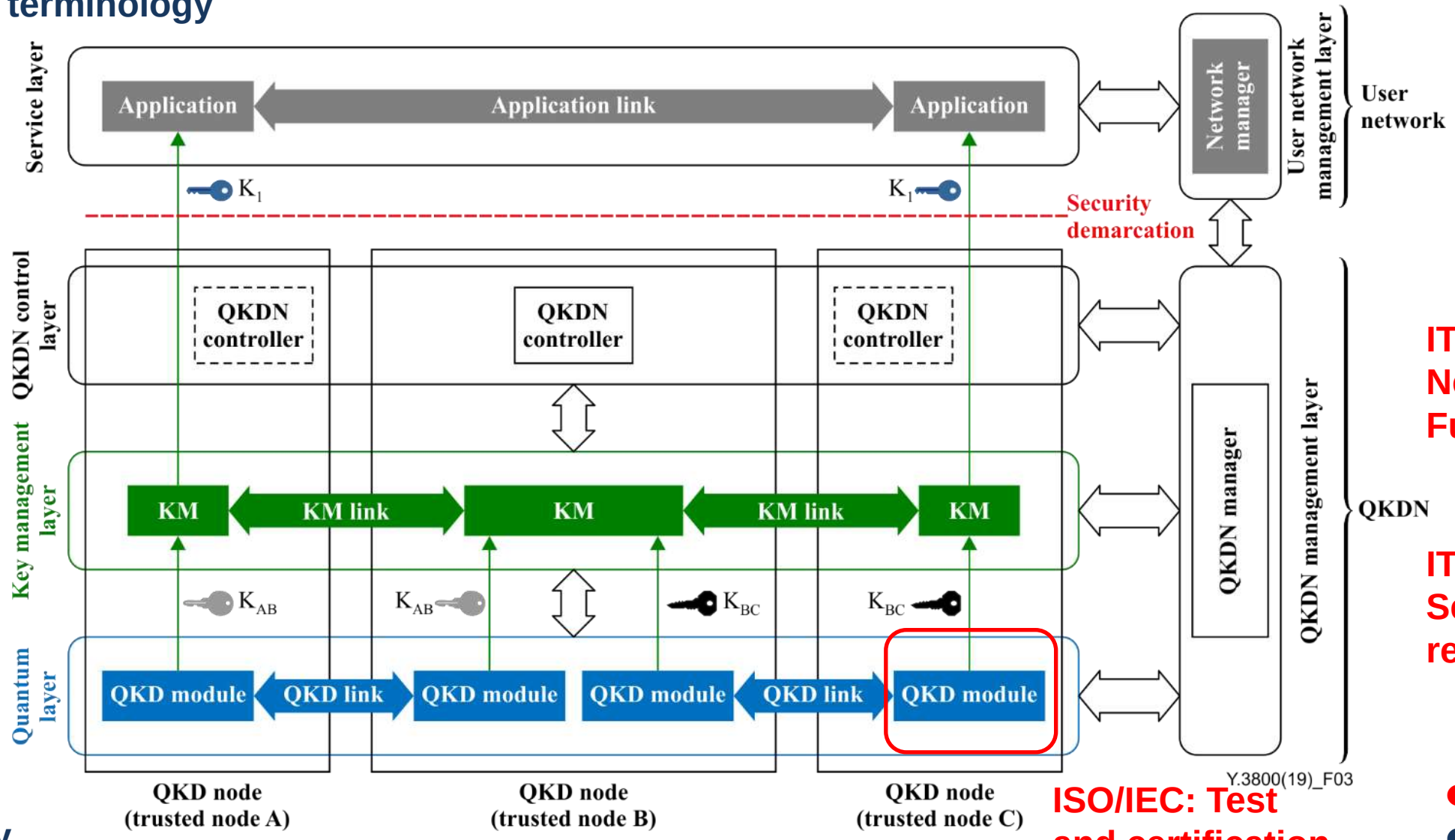
Standardization aspects in QKDN based on trusted nodes

FG QIT4N: terminology

FG QIT4N: use cases

FG QIT4N: Classical protocols

FG QIT4N: QKD protocols, transport technology



ITU-T SG 13: Network arch. Functions; QoS

ITU-T SG 17: Security requirements

ISO/IEC: Test and certification

- Standards
- Pre-study

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

Standardization activities in ISO/IEC JTC1 SC27 WG3

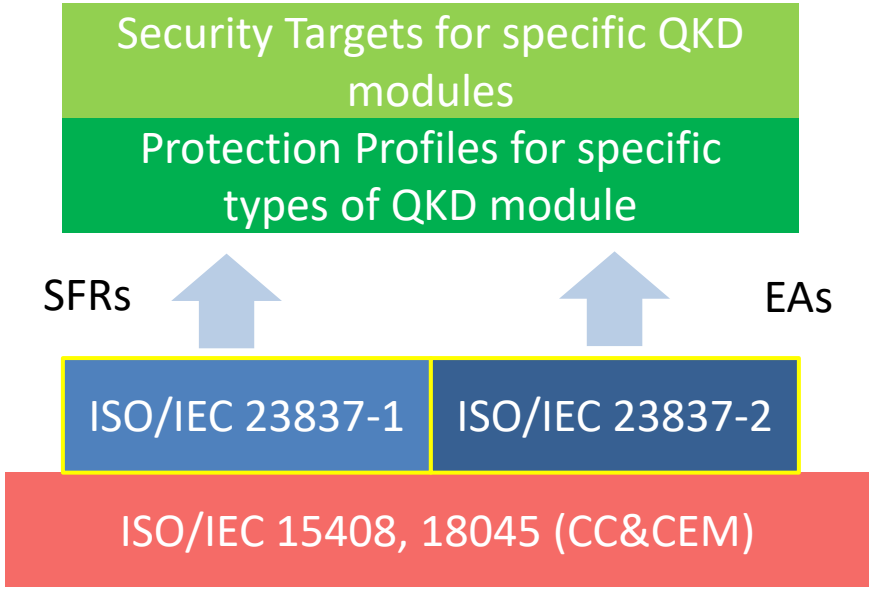
- **ISO/IEC 23837**: Security requirements, test and evaluation methods for quantum key distribution
  - Part 1: Requirements
  - Part 2: Test and evaluation methods

- Work item initiated in 2018 with one year preliminary study in 2017, currently under development

- Address QKD implementation security issues

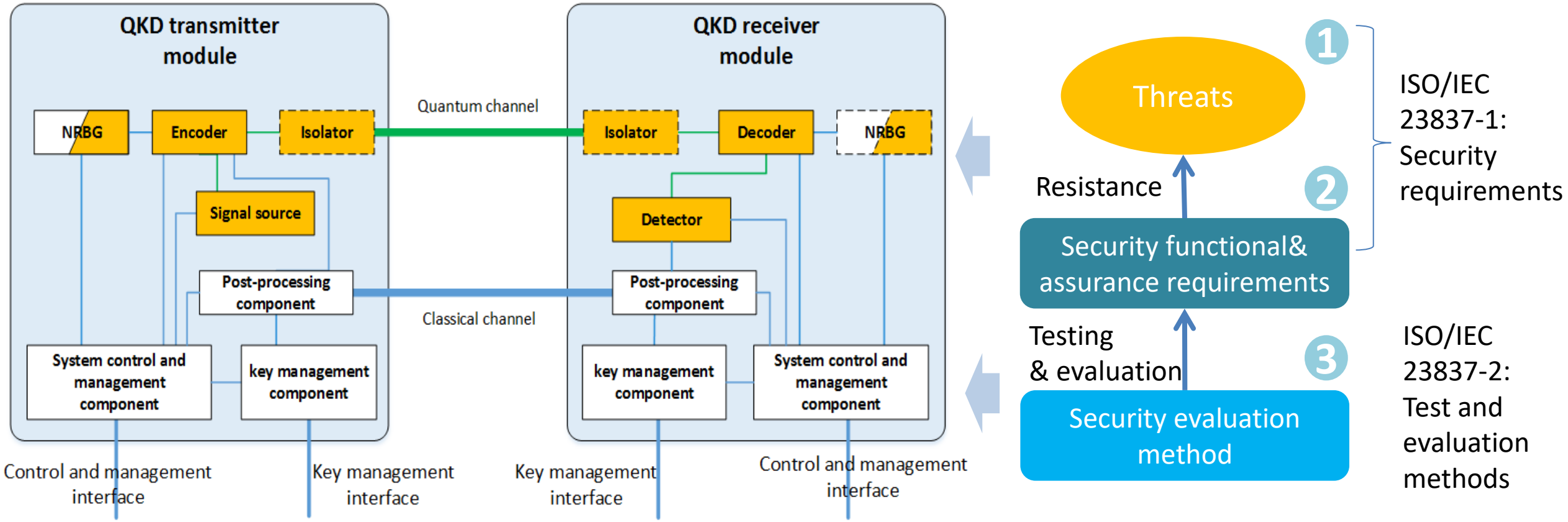
- High-level framework for the security evaluation of QKD module under the Common Criteria (CC) (ISO/IEC 15408) framework

https://www.iso.org/standard/77097.html
https://www.iso.org/standard/77309.html



- A baseline of Security Functional Requirements (SFRs), and relevant evaluation activities (EAs) for SFRs and SARs, and serve as a basis for developing relevant PPs/STs
- EAs for functional conformance test and vulnerability assessment (up to EAL5+AVA_VAN.5)

Standardization activities in ISO/IEC JTC1 SC27 WG3



Standardization activities in ITU-T SG 13

Study group 13: Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures

#	Work item	Name	Timing	Question
1	Y.3800	Framework for Networks to supporting Quantum Key Distribution	**Published** 2019-10	Q16
2	Y.3801	Functional requirement of the Quantum Key Distribution network	**Published** 2020-05	Q16
3	Y.3802	Functional architecture of the Quantum Key Distribution network	Consented 2020-07	Q16
4	Y.3803	Key management for Quantum Key Distribution network	Consented 2020-07	Q16
5	Y.3804	Control and Management for Quantum Key Distribution Networks	Consented 2020-07	Q16
6	Y.QKDN_SDNC	Software Defined Network Control for Quantum Key Distribution Networks	2021-09	Q16
7	Y.QKDN_BM	Business role-based models in Quantum Key Distribution Network	2021-03	Q16
8	Y.QKDN_frint	Framework for integration of QKDN and secure network infrastructures	2021-07	Q16

Arch., Framework, Functions related

#	Work item	Name	Timing	Question
9	Y.QKDN-qos-req	Requirements for QoS Assurance of the Quantum Key Distribution Network	2021-10	Q6
10	Y.QKDN-qos-gen	General Aspects of QoS (Quality of Service) on the Quantum Key Distribution Network	2021-10	Q6
11	Y. QKDN-qos-fa	Functional architecture of QoS assurance for quantum key distribution networks	2021-12	Q6
12	Y. QKDN-qos-ml-req	Requirements of machine learning based QoS Assurance for quantum key distribution networks	2022-07	Q6

Quality of service related

Q6: Quality of service (QoS) aspects including IMT-2020 networks
Q16:Knowledge-centric trustworthy networking and services

https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx

Standardization activities in ITU-T SG 17

Study Group 17: Security

#	Work item	Name	Topic	Timing	Question
1	X.1702	Quantum Noise Random Number Generator Architecture	QRNG	**Published** 2019-11	Q4(Cybersecurity)
2	X.sec_QKDN_ov	Security Requirements for QKD Networks – Overview	Security Req.	2020-08	Q4
3	X.sec_QKDN_km	Security Requirements for QKD Networks - Key Management	Security Req.	2020-08	Q4
4	X.cf_QKDN	Key combination and confidential key supply for quantum key distribution networks	Security app.	2020-08	Q4
5	X.sec_QKDN_tn	Security requirements for Quantum Key Distribution Networks-Trusted node	Security Req.	2021-03	Q4
6	TR.sec_QKD	**Tech. Report**: Security considerations for Quantum Key Distribution network	Security study	**Published** 2020-03	Q4

https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

PRE-standardization activities in ITU-T QIT4N

ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)

- Pre-study and pre-standardization
  - Gap analysis, status review, standardization analysis, future suggestions
  - Technical reports with NO normative contents

- Open platform for academic, industry, governments etc.
  - Established in 2019-10
  - 1 onsite meeting in Jinan, China; 4 E-meetings

  - WG1: Network aspects of QIT
  - WG2: QKD network

https://www.itu.int/en/ITUT/focusgroups/qit4n/Pages/default.aspx

FG QIT4N WG2:QKDN

Sub-group	Name	Current Version
D2.1	QIT4N terminology part 2: quantum key distribution network	QIT4N-O-048
D2.2	Technical report on the QIT4N use case part 2: quantum key distribution network	QIT4N-O-049
D2.3	Technical report on QKDN protocols Part1:Quantum layer Part2: Classical layers	QIT4N-O-050&51
D2.4	Technical report on QKDN transport technologies	QIT4N-O-052
D2.5	Technical report on QIT4N standardization outlook and technology maturity part 2: quantum key distribution network	QIT4N-O-053

Participations

- Main contributors from China, Japan, Korea, Switzerland, UK, US etc.

.....

ISO

- Restricted to experts from each country's national body channel

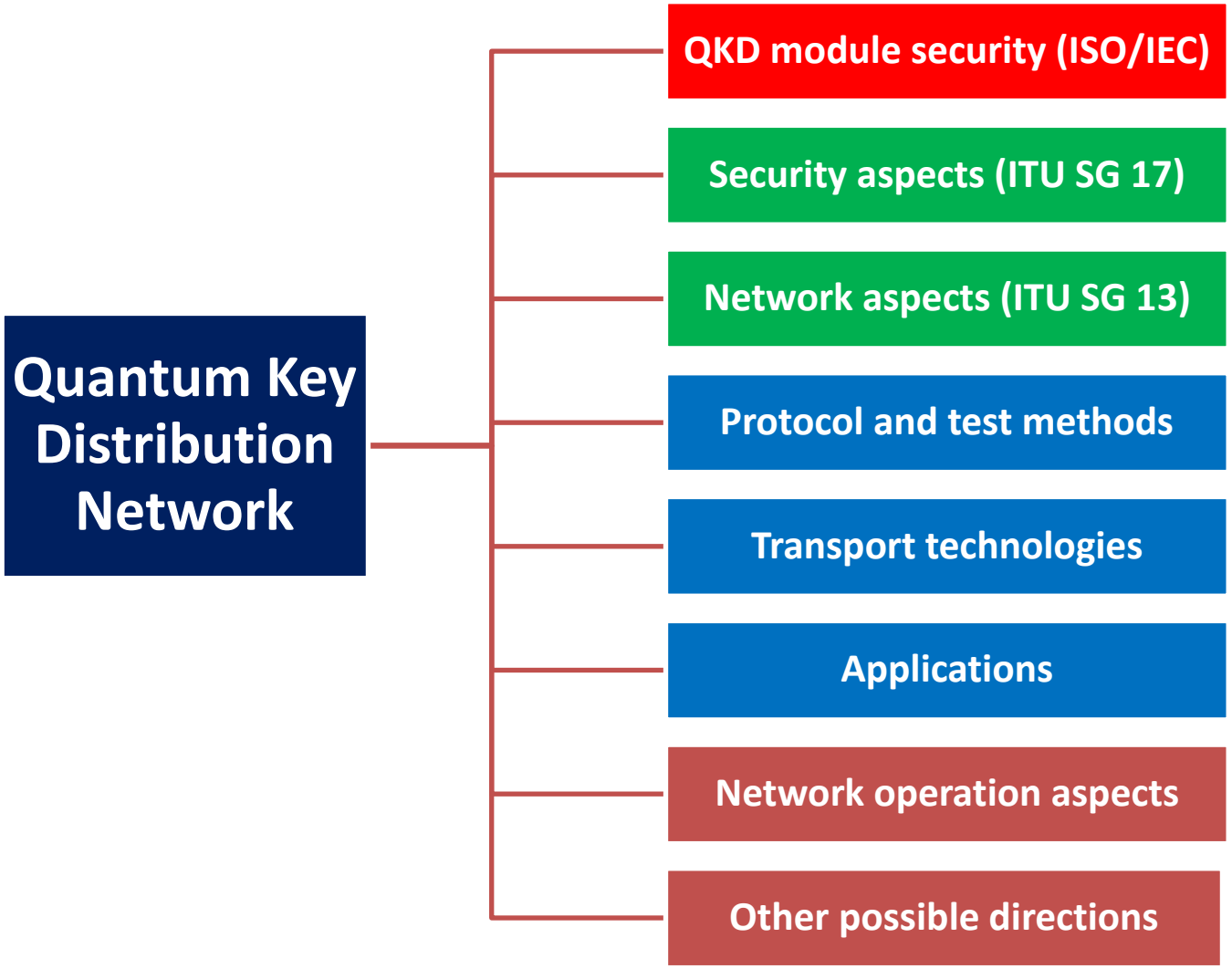
ITU

- Study groups: Membership based
  Activities in study groups with different topics
- Focus group: open for everyone
  Free of charge, new comer friendly, flexibility, wide range of topics

➢ Liaison channels among different SDOs

Gap analysis and possible future works

Ongoing studies in ISO/IEC; ITU-T study groups, FG-QIT4N
Potential future studies in SDOs



ISO IEC

ITU ETSI World Class Standards

IETF IEEE


Thanks.