ITU KALEIDOSCOPE
ONLINE 2021

6-10 December 2021

Quantum key distribution networks for trusted 5G and beyond: An ITU-T standardization perspective

Taesang Choi, (ETRI, Korea); Hyungsoo Kim (KT, Korea);
Jeongyun Kim (ETRI, Korea); Chun Seok Yoon (KT, Korea);
Gyu Myoung Lee (Liverpool John Moores University, UK and KAIST, Korea)

Taesang CHOI
Electronic and Telecommunications Research Institute (ETRI)

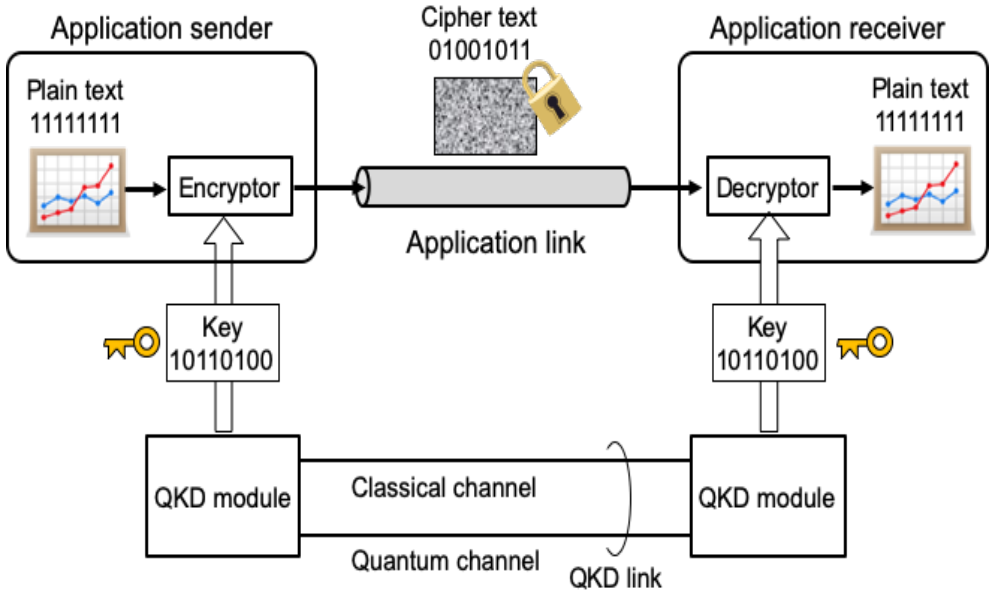
Session: Invited paper

Contents

Introduction

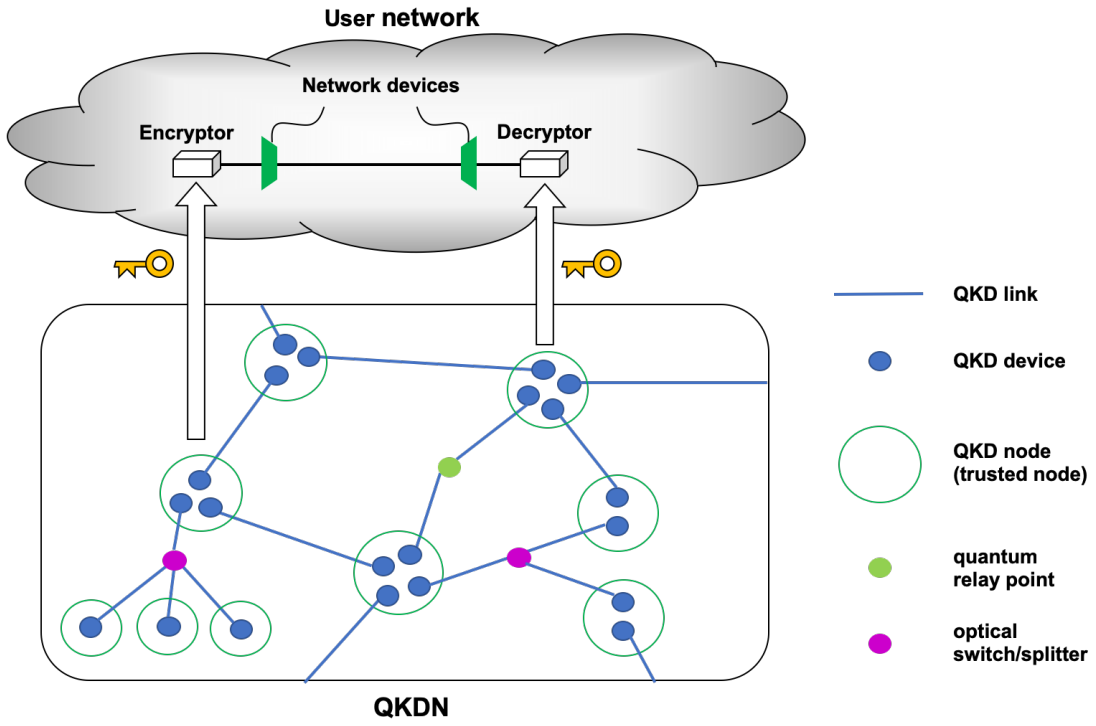
- Quantum Key Distributions (QKD)
  - procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory (by ETSI)
- From QKD system to QKD network

- Related standardization bodies
  - ITU-T
  - ETSI ISG QKD
  - ISO/IEC JTC1/SC27
  - IETF/IRTF – Quantum Internet Research Group

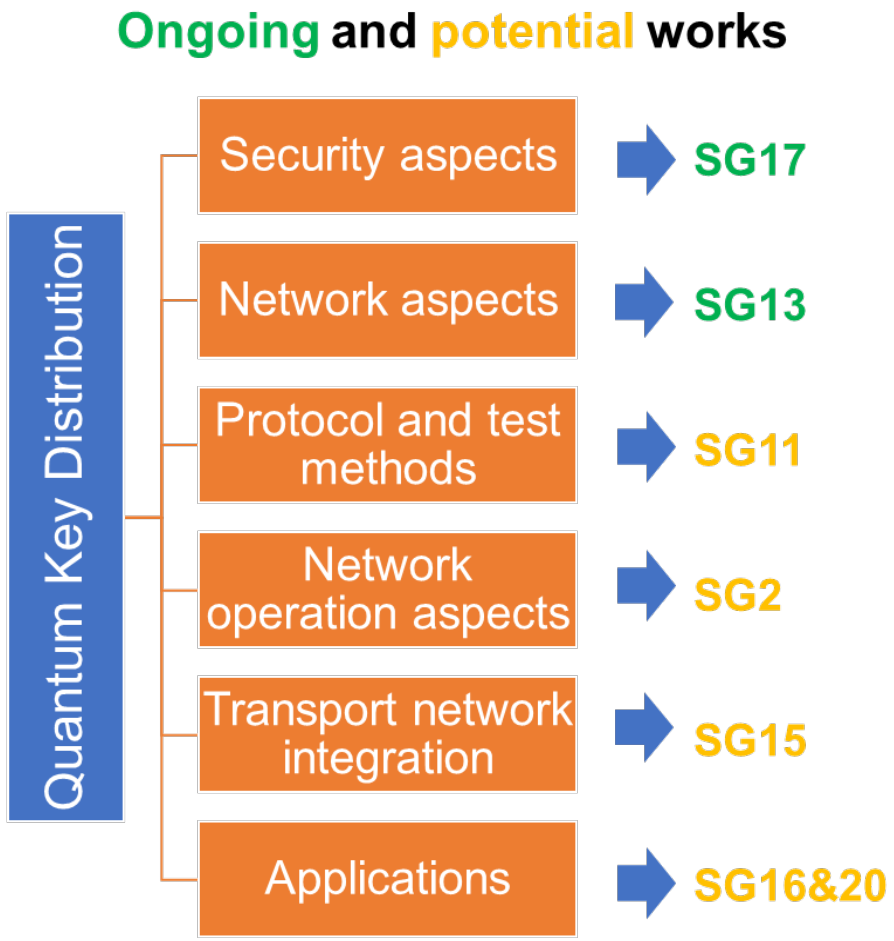


QKDN standardization in ITU-T

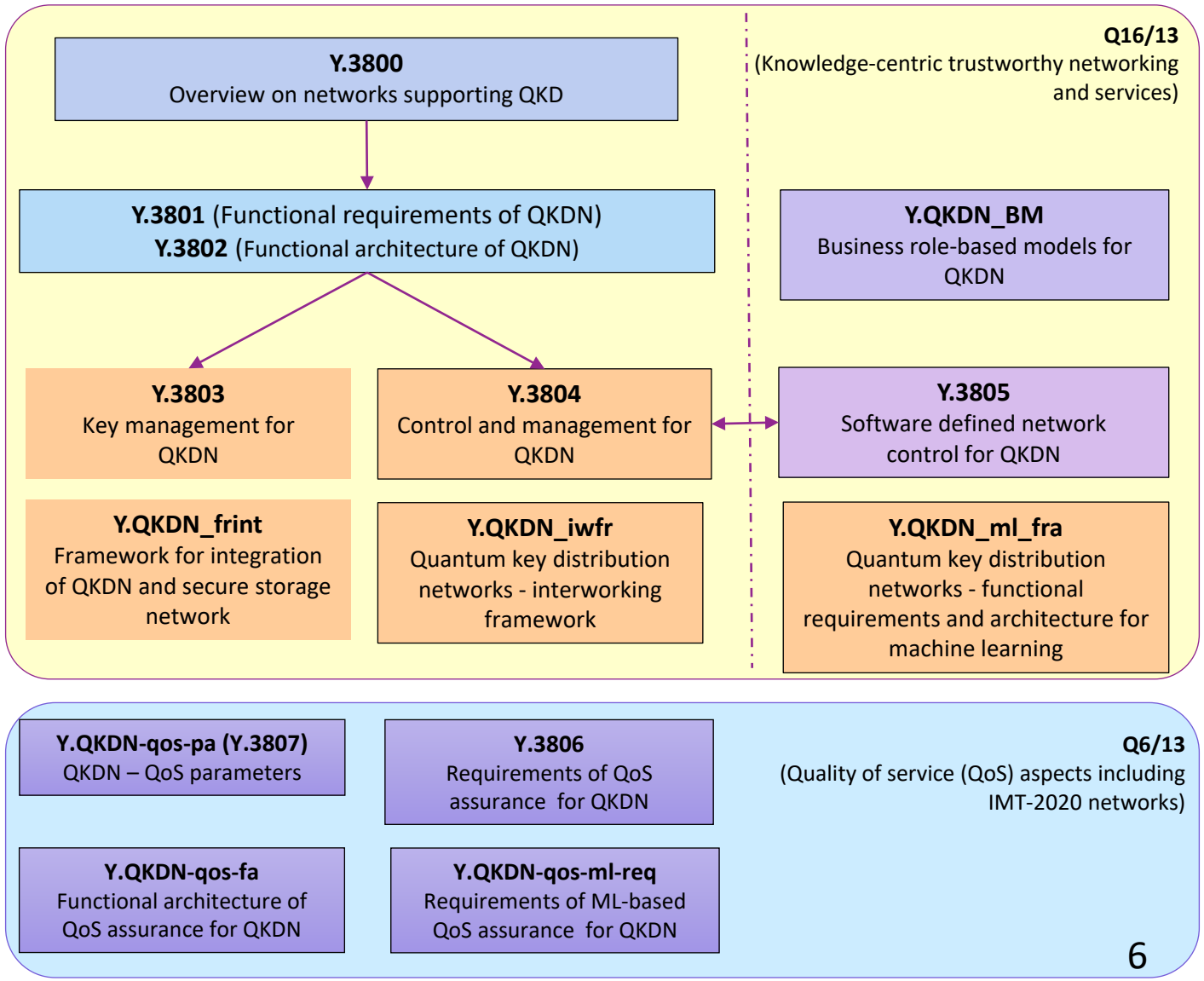
- QKDN concepts and their relation to a user network



- QKDN standardization aspects in the context of ITU-T



Standardization for QKDN in ITU-T SG13/17/11



Q4/17
(Quality of service (QoS) aspects including IMT-2020 networks)

X.sec_QKDN_km
Security requirements for QKDNs – key management

X.sec_QKDN_tn
Security requirements for QKDNs – trust node

X.sec_QKDN_intrq
Security requirements for QKDNs – Infra integration

X.sec_QKDN_CM
Security requirements for QKDNs – control and management

X.sec_QKDN_AN&AZ
Security requirements for QKDNs – authentication and authorization

Q2/11
(Signalling requirements and protocols for services and applications in telecommunication environments)

Q.QKDN_sig_cm
Signaling requirements and protocols for QKDN control and management

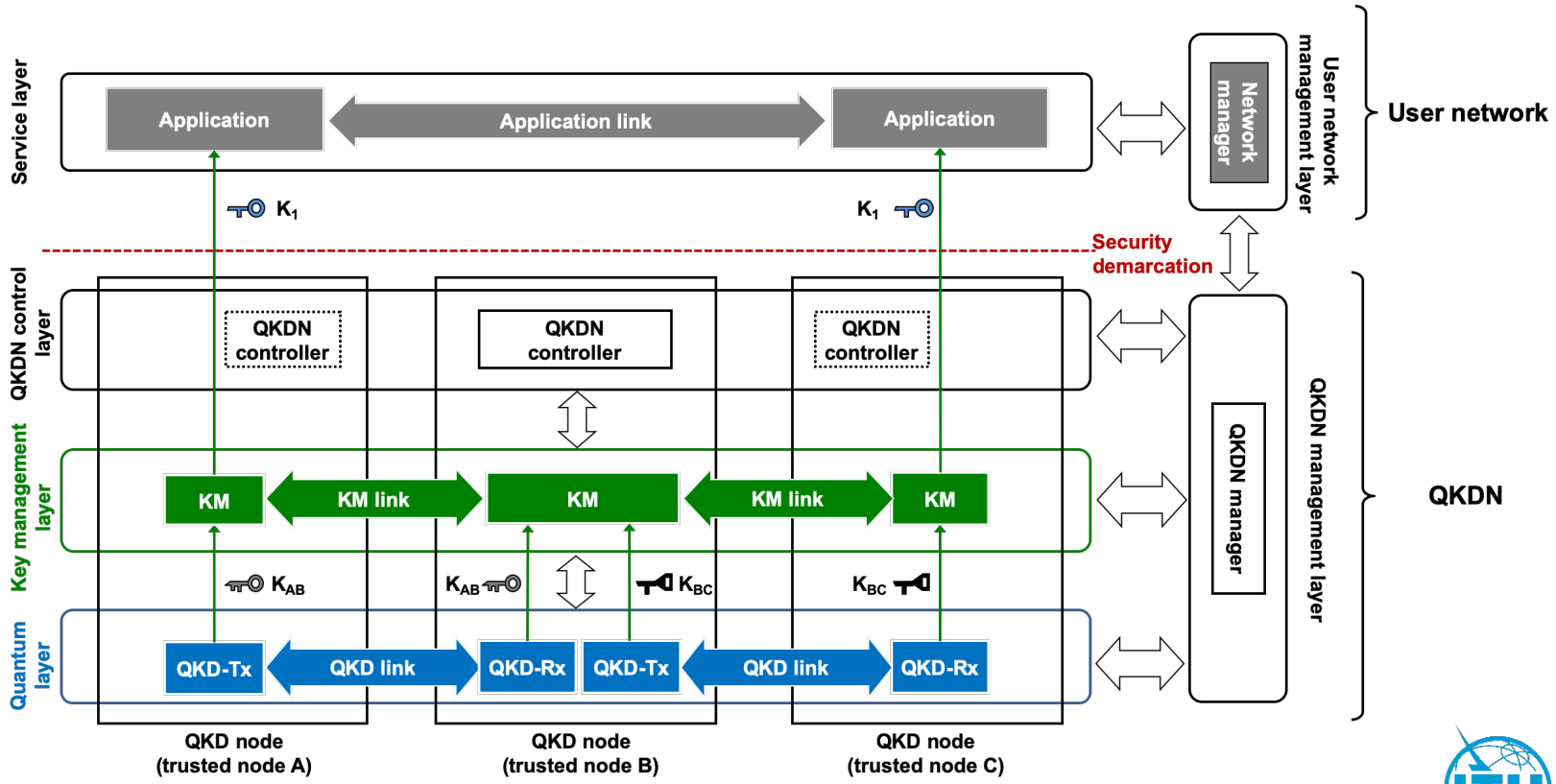
Q.QKDN_profr
Framework for QKDN Protocols

Y.3800: overview on QKDN

- This Recommendation specifies an overview on networks to support quantum key distribution (QKD) to address network aspects to implement QKD technologies.
  - an overview of QKD technologies;
  - network capabilities to support QKD;
  - Conceptual structure and basic functions of QKD networks (QKDN).

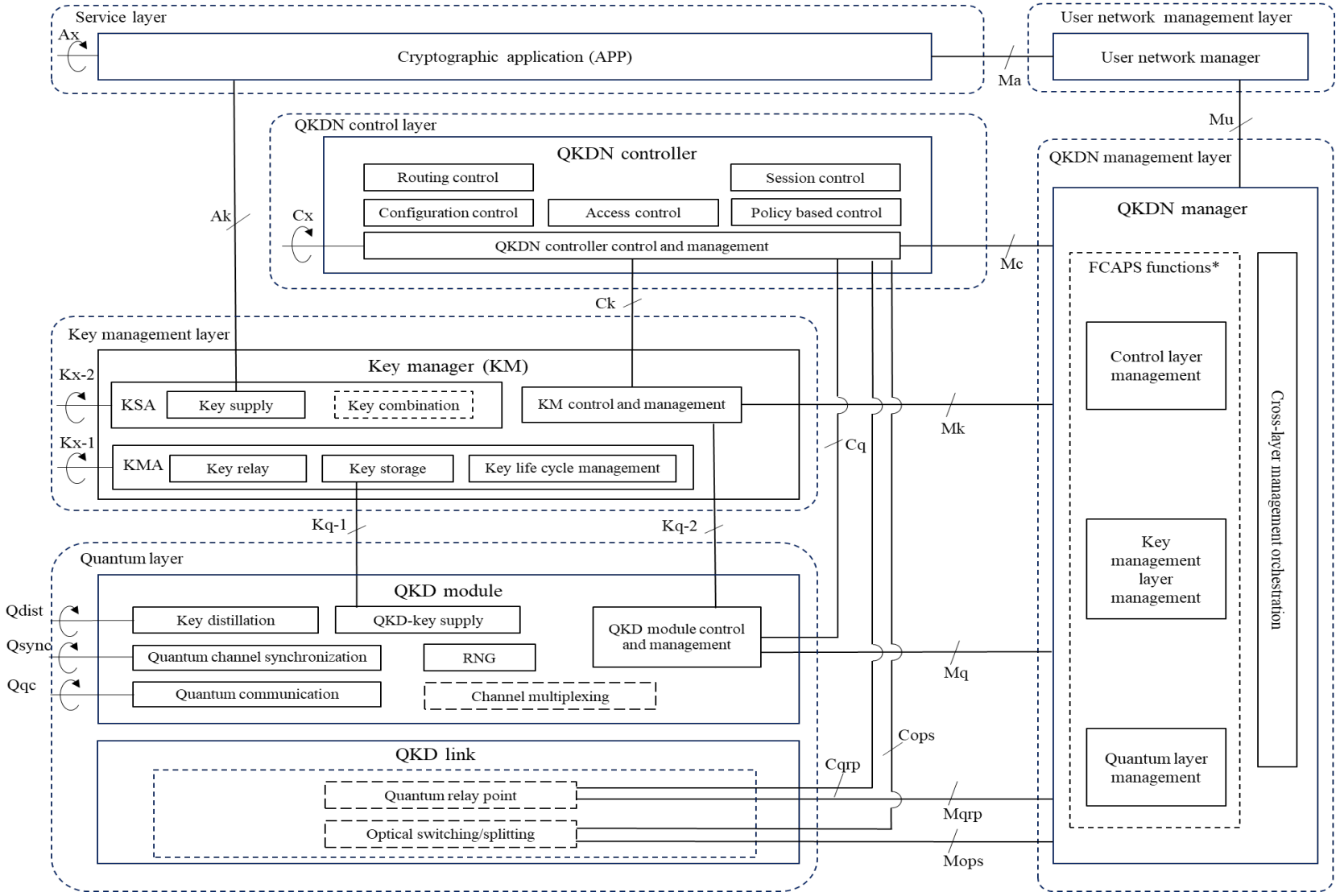
Y.3801: QKDN – Functional requirements

- This Recommendation is to specify functional requirements for QKDN:
  - Functional requirements for capabilities of quantum/key management/QKDN control and management layers and other capabilities for QKDN



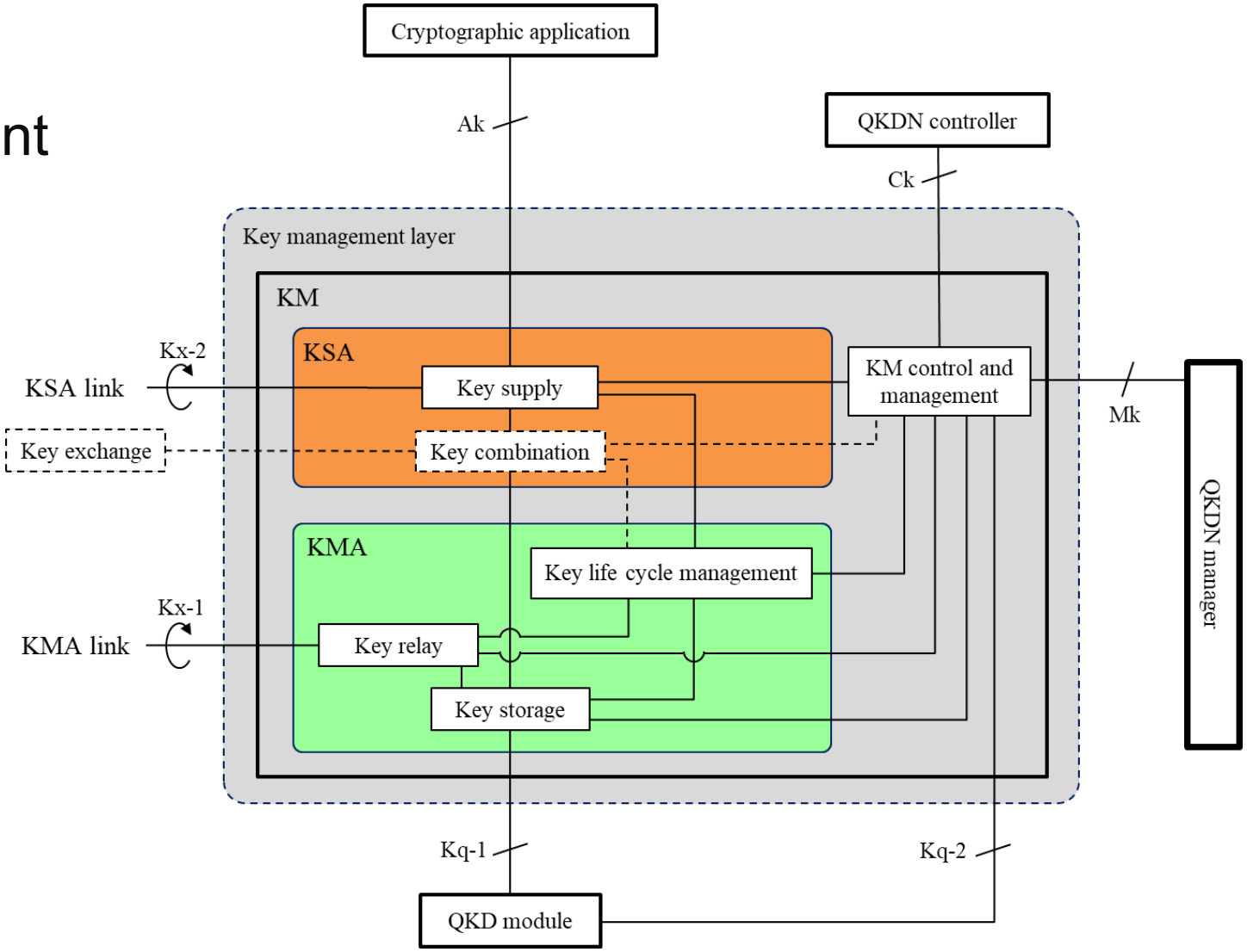
Y.3802: QKDN – functional architecture

- This Recommendation specifies functional architectures of the QKDN.
  - Functional architecture model
  - Functional elements and reference points
  - Architectural configurations
  - Overall operational procedures



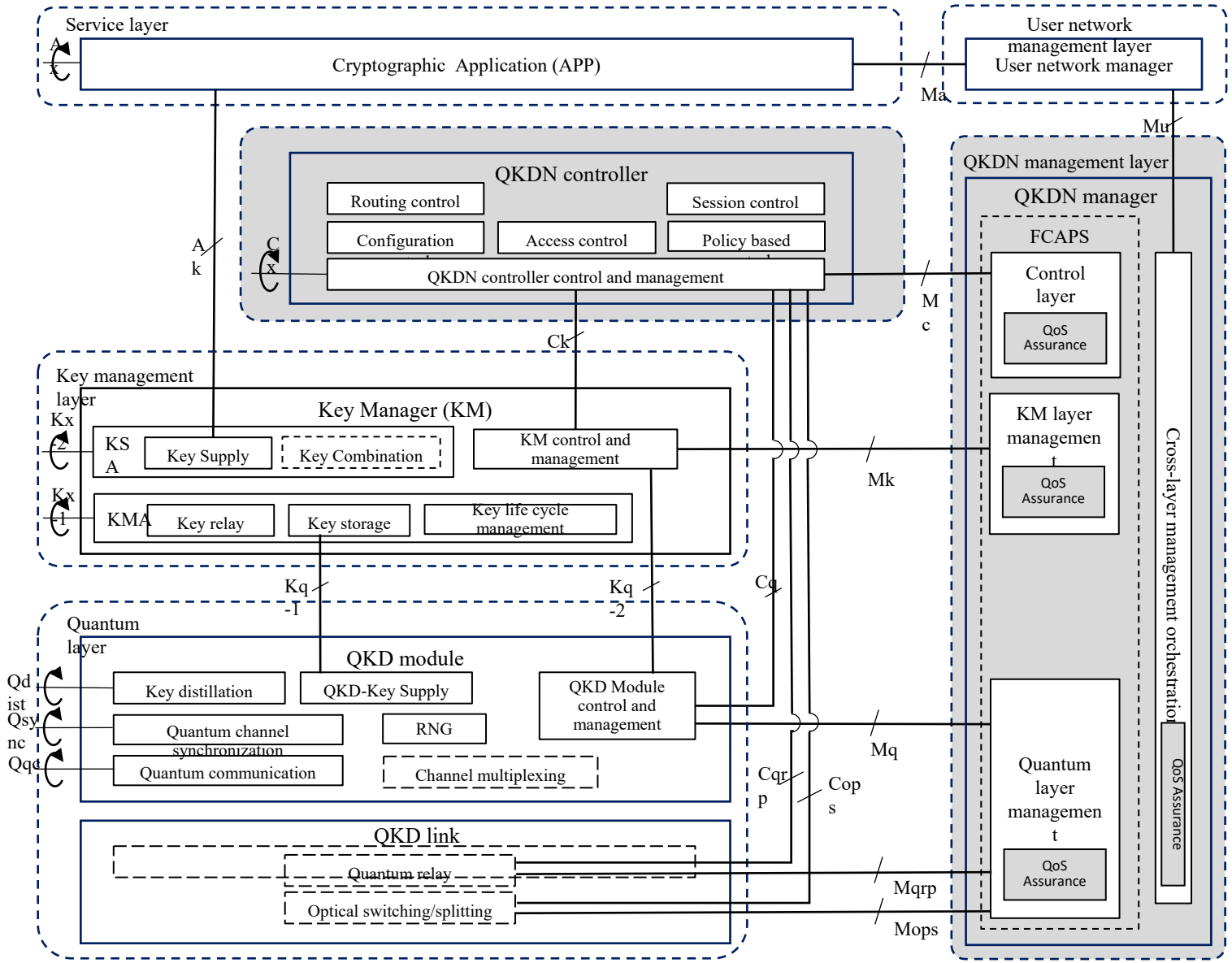
Y.3803: QKDN – Key management

- This Recommendation describes key management for QKDN which addresses technical specifications to help the implementation and operation.
  - Requirements of key management
  - Functional elements of key management
  - Procedures of key management
  - Key formats (key data and meta-data)



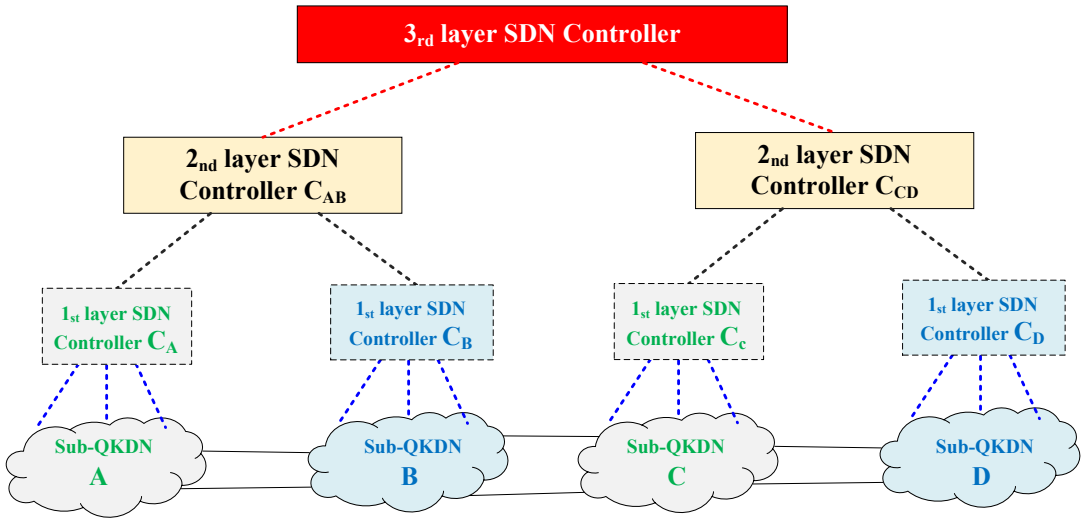
Y.3804: QKDN – Control and management

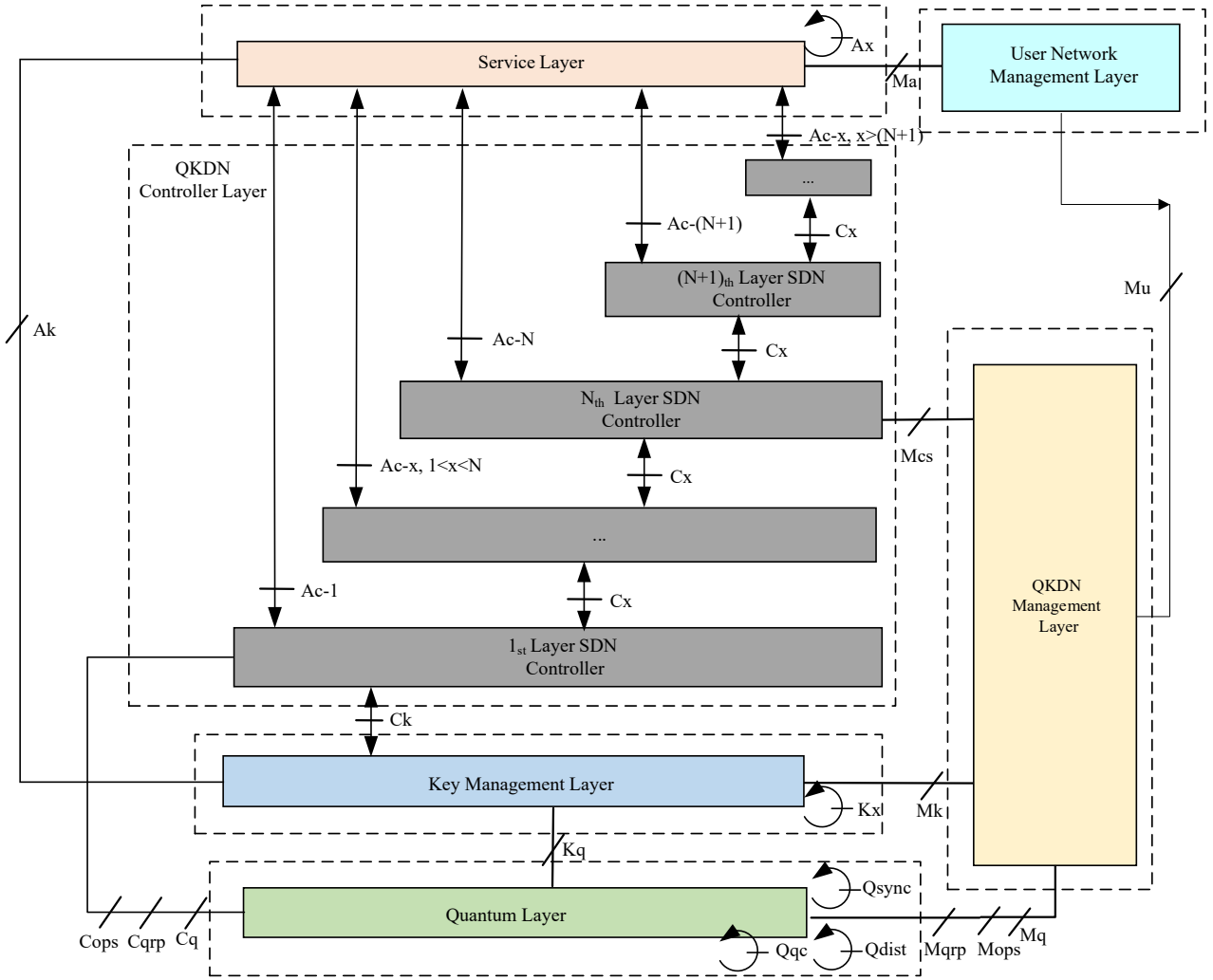
- This Recommendation is to specify the control, management, and orchestration for QKDN
  - Functional requirements of QKDN control, management, and orchestration
  - Management information model for QKDN
  - Reference points of QKDN control, management, and orchestration
  - Procedures of QKDN control, management, and orchestration



Y.3805: QKDN – Software Defined Networking Control

- This Recommendation covers:
  - Requirements for SDN control in QKDN;
  - Functional architecture of SDN control in QKDN;
  - Reference points of SDN control in QKDN;
  - Hierarchical SDN controller in QKDN;
  - Overall operational procedures of SDN control in QKDN



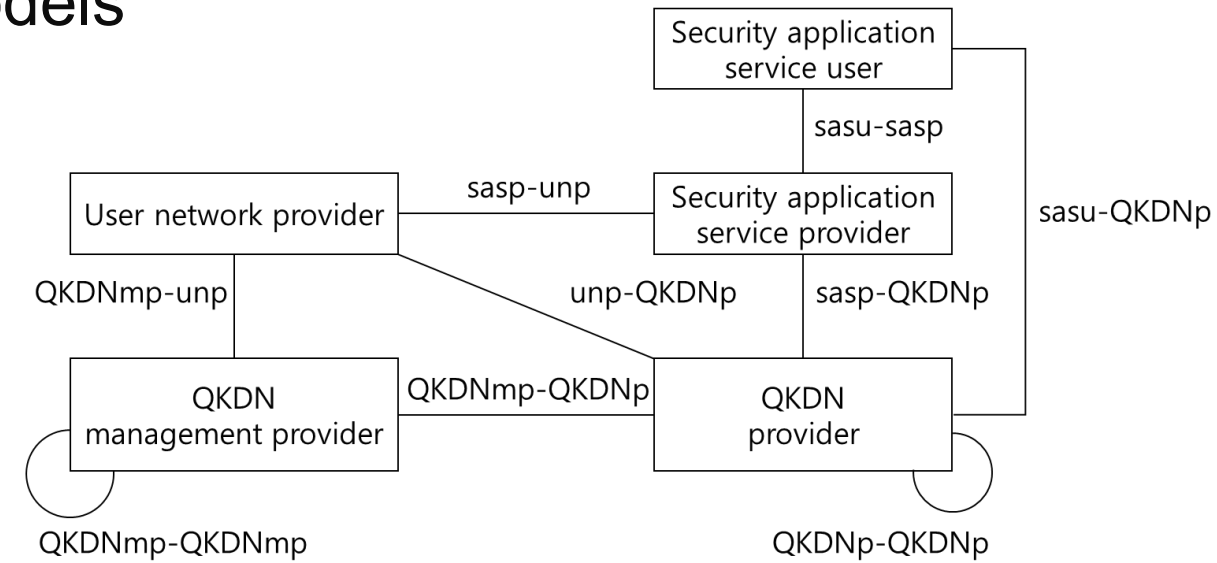


On-going work items on QKDN in ITU-T SG13

SG/Q	Work item
Q16/13	Y.QKDN_BM : Quantum key distribution networks – Business role-based models
	Y.QKDN_frint : Framework for integration of QKDN and secure storage network
	Y.QKDN-iwfr : Quantum key distribution networks – interworking framework
	Y.QKDN-ml-fra : Quantum key distribution networks – Functional requirements and architecture to enable machine learning
	Y.QKDN-rsfr : Quantum key distribution networks – resilience framework
	Y.supp.QKDN-roadmap : Standardization roadmap on Quantum Key Distribution Networks
Q6/13	Y.QKDN-QoS-pa: Quantum key distribution networks – QoS parameters
	Y.QKDN-QoS-fa: Functional architecture of QoS assurance for quantum key distribution networks
	Y.QKDN-QoS-ml-req: Requirements of machine learning based QoS assurance for quantum key distribution networks

Y.QKDN_BM: Business role-based models

- Y.QKDN_BM describes business roles, business role-based models, and service scenarios in a QKDN from different deployment and operation perspectives.
- Especially, Y.QKDN_BM identifies various business models that require security application services with a QKDN and exiting user networks.

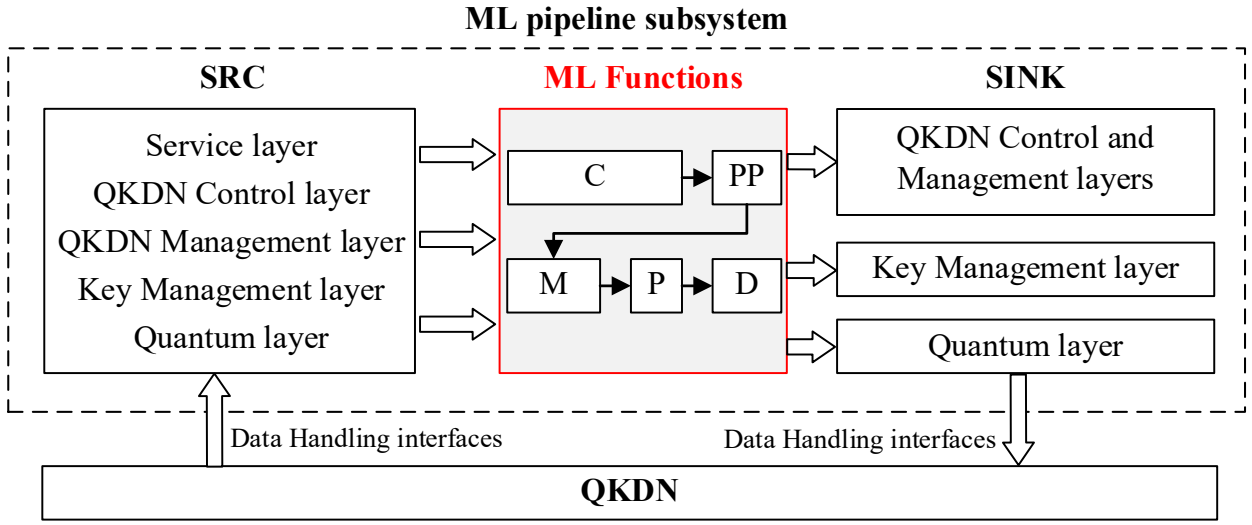


Y.QKDN_frint: Integration of QKDN and secure storage network

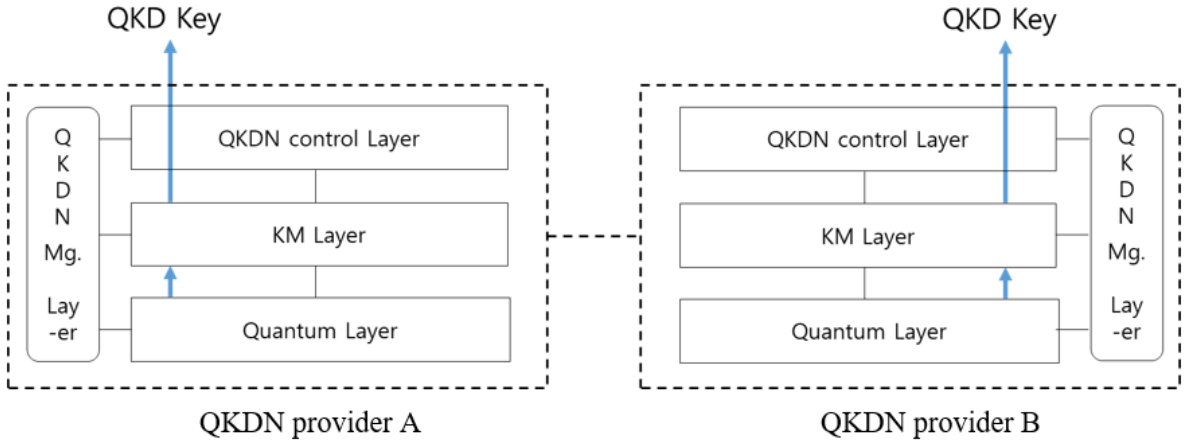
- This Recommendation describes framework for integrating QKDN and secure storage network (SSN).
  - functional requirements for SSN;
  - functional architecture model of SSN;
  - reference points;
  - operational procedures;
  - phase-in scenarios.

Recently started work items

- Y.QKDN-iwfr
  - Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other.
  - It mainly focuses on the interworking between QKDNs supported by multiple QKDN providers.
- Y.QKDN-ml-fra
  - For the functional requirements and architectures for a ML-enabled QKDN, it specifies the roles of ML in a QKDN.
  - It includes functional requirements and a functional architecture model of the ML-enabled QKDN.
- Y.QKDN-rsfr
  - It specifies the framework of resilience in a QKDN including the conceptual models of QKDN protection and recovery scenarios.
  - It also provides typical use cases of resilience and related requirements of resilience schemes supported by the quantum layer, the key management layer, and QKDN control and management layers, respectively.

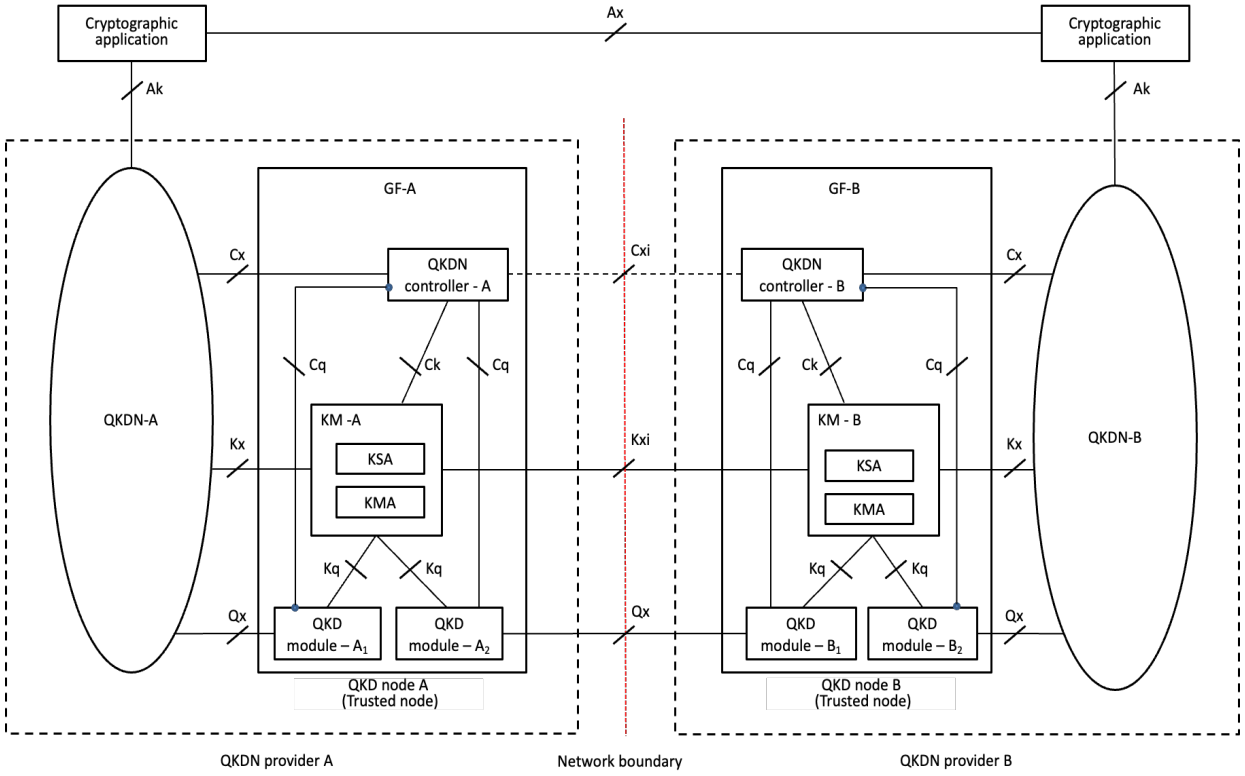


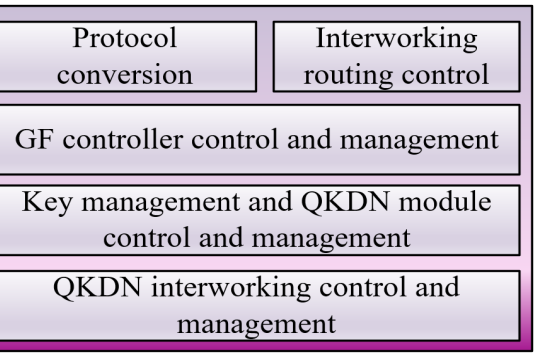
C: collector; PP: preprocessor; M: model; P: policy; D: Distributor; SRC: source of data; SINK: target of ML output



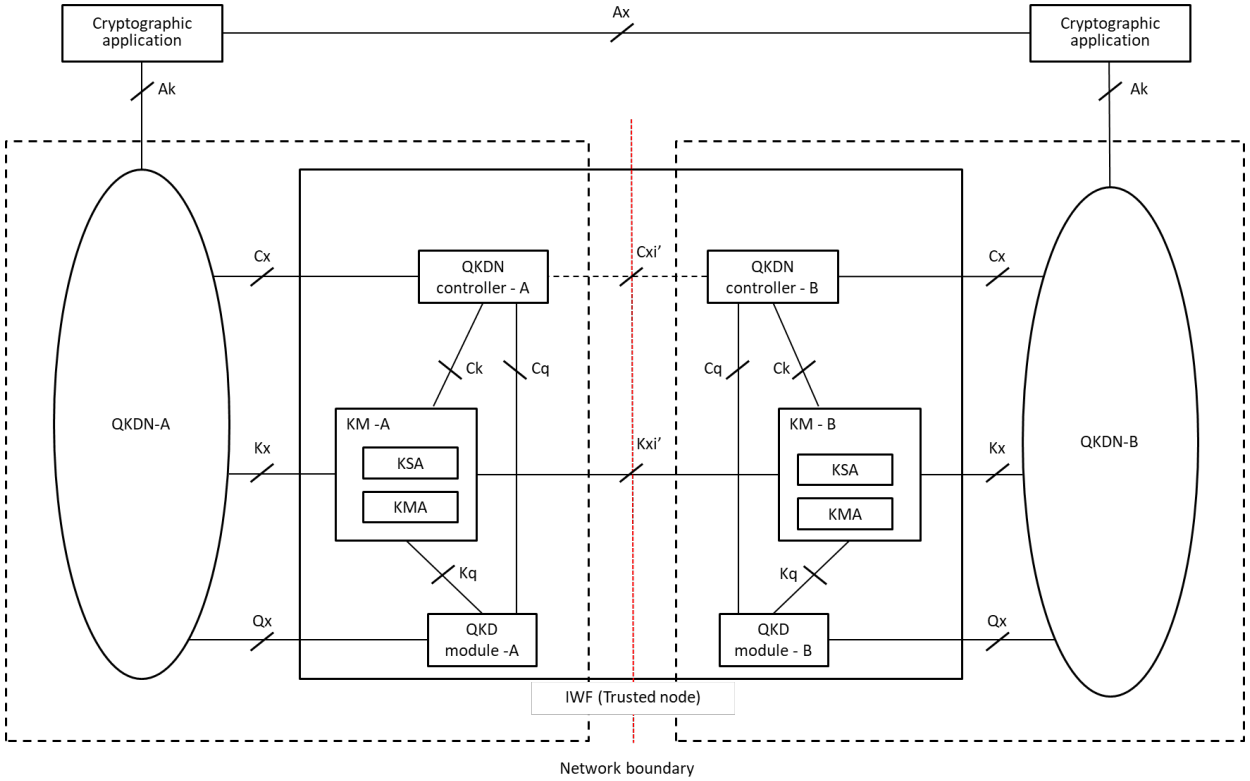
QKDNs Interworking Scenarios

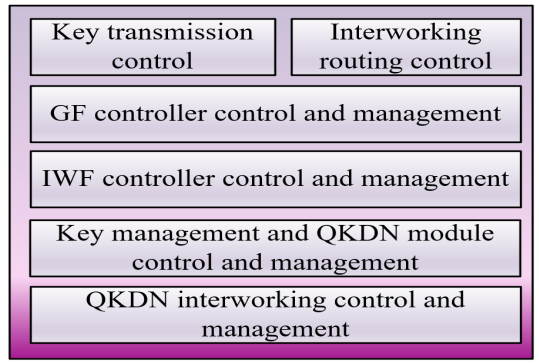
Scenario 1 – Interworking of QKDNs with GFs





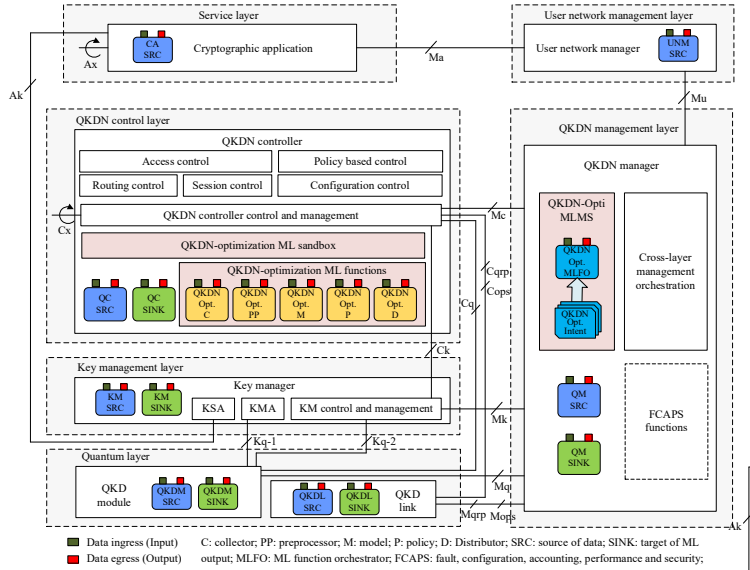
Scenario 2 – Interworking of QKDNs with IWFs



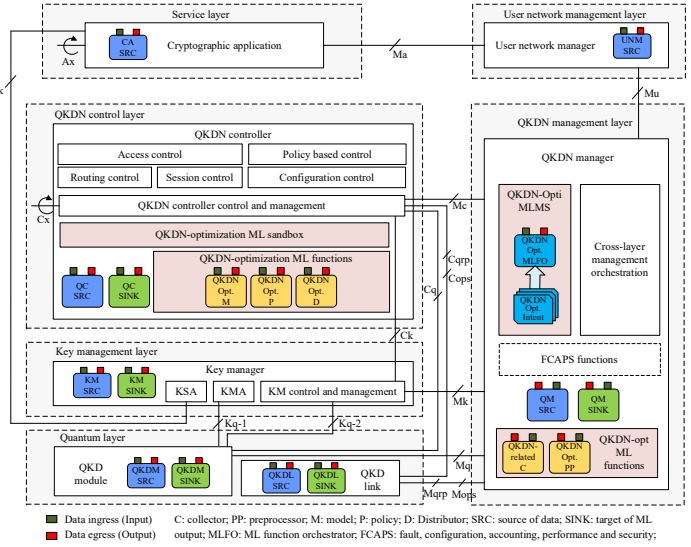


Architectural Variations of ML-enable QKDN

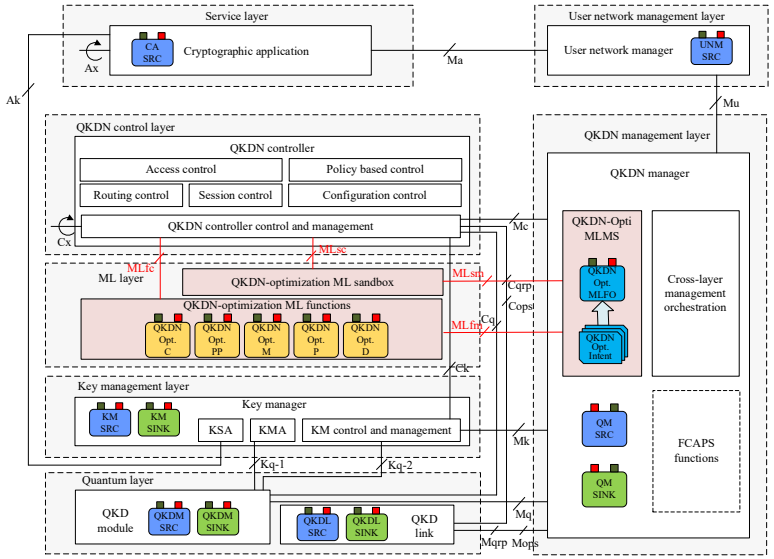
Strategy A (QKDN-optimization ML functions are all located in QKDN controller)



Strategy B (QKDN-optimization ML functions are distributed in QKDN controller and QKDN manager)



Strategy C (QKDN-optimization ML functions and ML sandbox are located in a new layer called ML layer)



ITU KALEIDOSCOPE ONLINE 2021

QoS aspects in QKDN

- Y.QKDN-QoS-pa
  - It covers the descriptions of QoS and network performance in a QKDN, classification of performance concerns for which parameters may be needed, QoS parameters of a QKDN and network performance supporting factors.

- Y.QKDN-QoS-fa
  - It gives an overview of QoS assurance for a QKDN, a functional architecture of QoS assurance for a QKDN, reference points of functional architecture and procedures of QoS assurance for a QKDN.

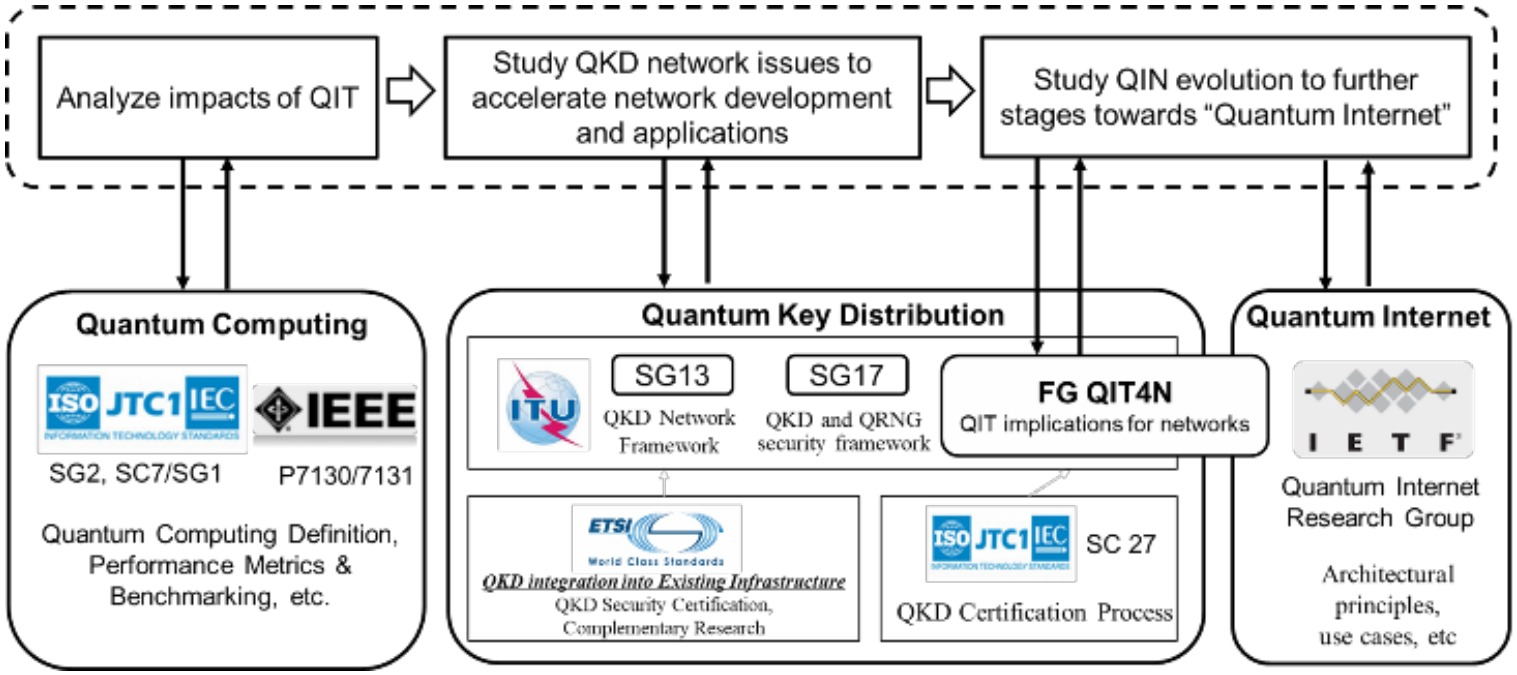
- Y.QKDN-QoS-ml-req
  - It first provides an overview of requirements of ML-based QoS assurance for QKDN. It also describes a functional model of ML-based QoS assurance and followed by associated high level and functional requirements of ML-based QoS assurance.

Standardization roadmap on QKDN

- Y.supp.QKDN-roadmap
  - It describes the landscape with related technical areas of trust technologies from an ITU-T perspective and list up related standards and publications developed in other SDOs.

Pre-standardization activities in ITU-T FG-QIT4N

- Quantum Information Network
  - Quantum Computing
  - Quantum Communication
  - Quantum Sensing & Metrology
- Quantum Information Technology
  - Telecom/network aspects of QKDNs: SG13 (QKDN architecture aspect), SG17 (security of QKDN and applications of QRNG for security)
  - QIN technology and network evolution.

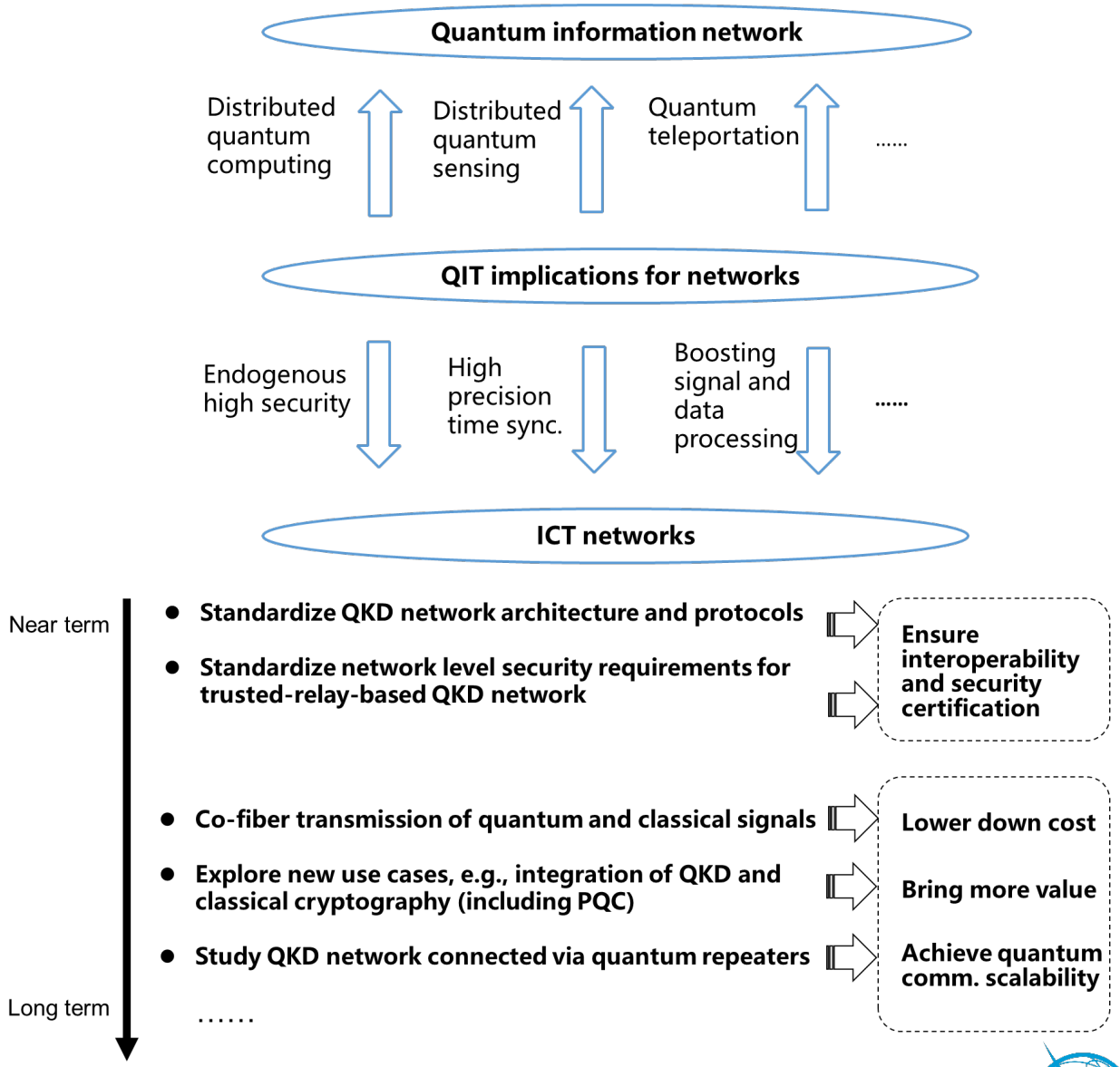


FG-QIT4N planned deliverables

WG	Deliverables	
WG0 (Coordination committee)	D0.1	QIT4N standardization landscape and outlook
WG1 (Network aspects of QIT)	D1.1	QIT4N terminology part 1: Network aspects of QIT
	D1.2	QIT4N use case part 1: Network aspects of QIT
	D1.3	Implications of quantum information technology on networks
	D1.4	QIT4N standardization outlook and technology maturity part 1: Network aspects of QIT
WG2 (QKDN)	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

Challenges as potential work items

- Support of QKDN interoperability
- Specifications of QKDN protocols
- Synchronization
- Multi-protocol connectivity
- The adoption of AI/ML to a QKDN
- Integration of user networks (e.g., 5G and beyond)
- Trusted-relay-based QKDN
- Scale up QKDN
- Towards QENS from QKDN



Conclusion

- Standardization activities in ITU-T SG13 and FG-QIT4N
  - The introduction of a QKDN into the current networks brings new challenges to the design of the network architecture and security considerations.
- Future standardization
  - Identified key challenges and potential work items for QENS
  - Considering trustworthy networking technologies and AI/ML techniques for cryptographic applications in 5G and beyond.
- For future work
  - Supporting trustworthy networking and services as well as cryptographic applications
  - Tightly integrating with 5G networks and beyond as user networks with QKD and QITs

ITU KALEIDOSCOPE
ONLINE 2021

Thank you!