Eighth SG13 Regional Workshop for Africa
“Standardization and Future Networks: Opportunities for Africa Beyond 2020”

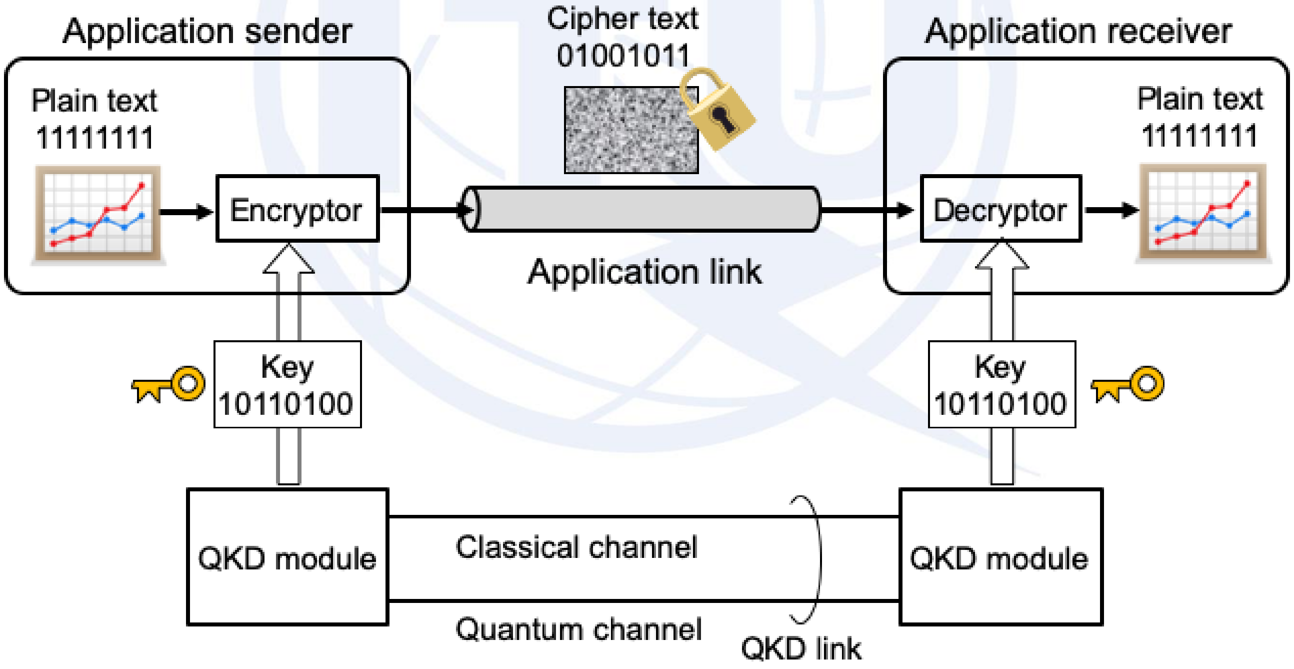
Standardization activities on Quantum Key Distribution Networks in ITU-T

1 June 2021

Gyu Myoung Lee
WP3/13 co-chair, Q16/13 Rapporteur
gmlee@kaist.ac.kr

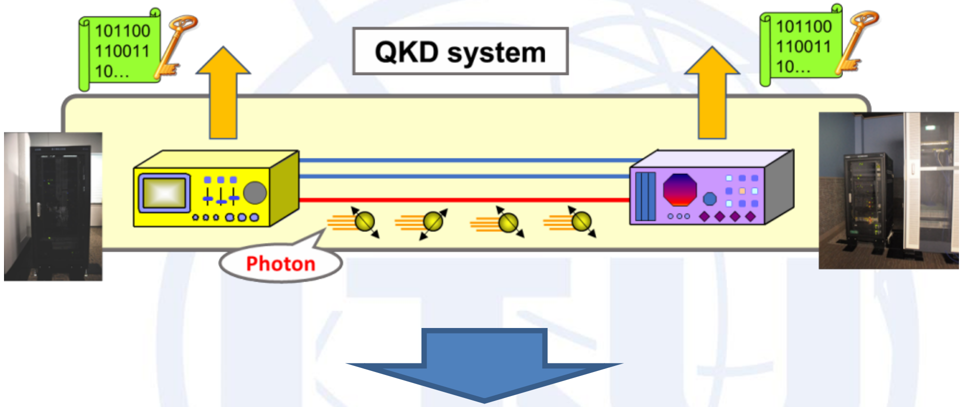
Quantum Key Distribution (QKD)

- procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory (by ETSI)

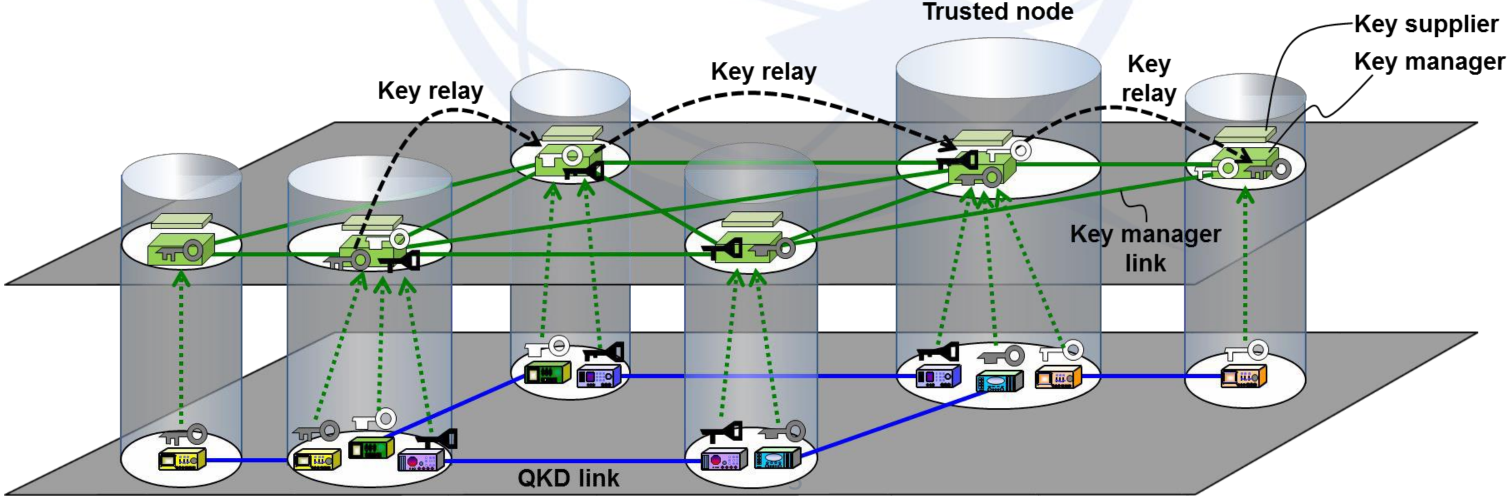


Configuration example of QKD use for securing a P-to-P application link

From QKD system to QKD network



QKD Network



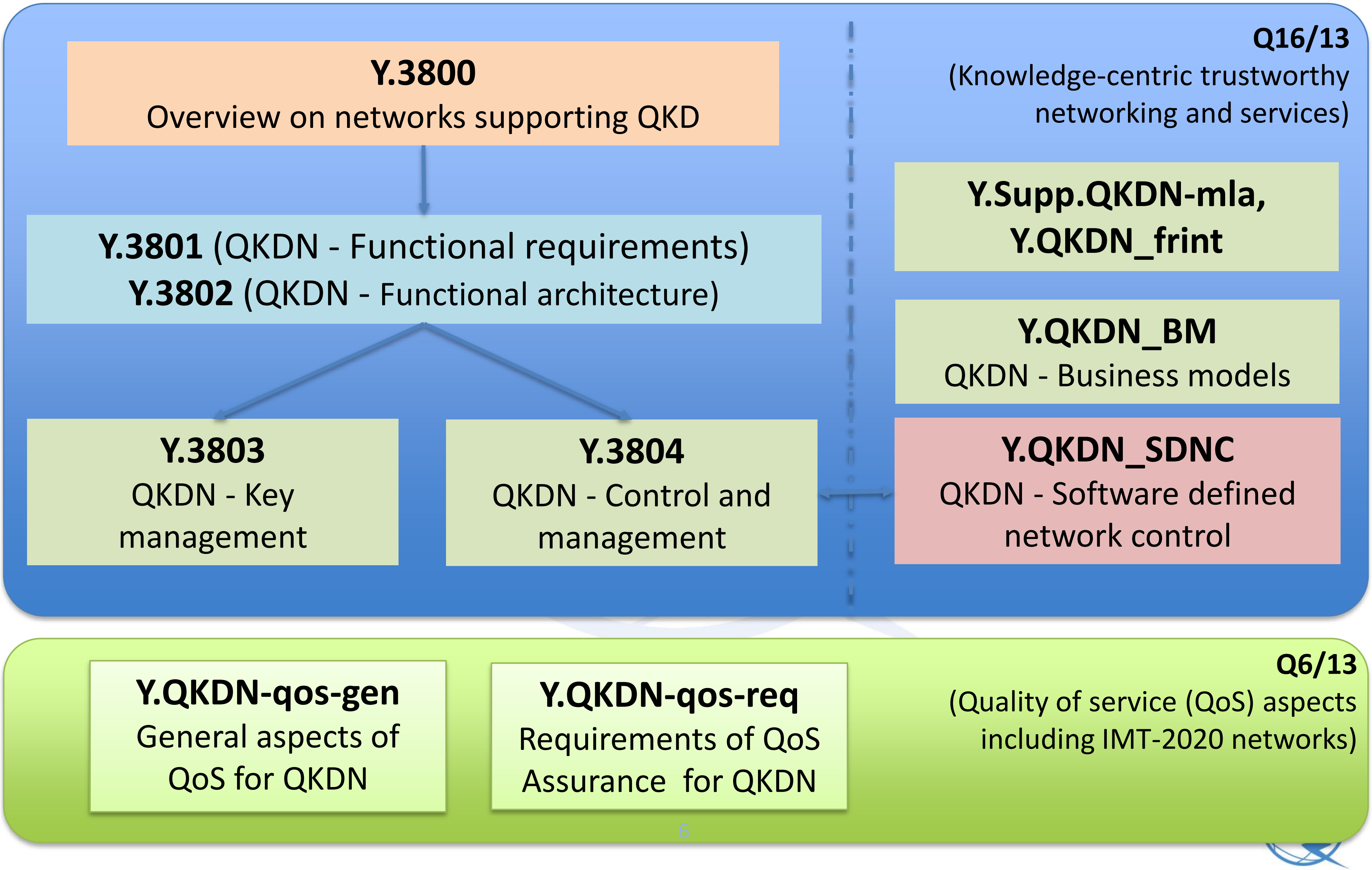
Progress of QKDN standardization in ITU-T SG13 (Q16/13) (1)

- July 2018
  - – First initiative on QKDN – Y.QKDN_FR
- March 2019
  - – Two new work items: Y.QKDN_Arch, Y.QKDN_KM
- June 2019
  - – First Rec. Y.3800 was consented
  - – Two new work items: Y.QKDN_CM, Y.QKDN_SDNC
- October 2019
  - – First Rec. Y.3800 (i.e., Y.QKDN_FR) was approved
  - – Four new work items: Y.QKDN-req, Y.QKDN-BM, Y.QKDN-qos-gen, Y.QKDN-qos-req

Progress of QKDN standardization in ITU-T SG13 (Q16/13) (2)

- March 2020
  - Corrigendum to Y.3800 and Y.3801(Y.QKDN-req) were consented
  - New work item: Y.supp.trust-roadmap
- July 2020
  - 3 Recs (Y.3802(Y.QKDN_Arch), Y.3803(Y.QKDN_KM) and Y.3804(Y.QKDN_CM)) were consented
  - New work item: Y.QKDN_frint
- December 2020
  - New work item: Y.Supp.QKDN-mla
- July 2021
  - Candidate documents for completion (Y.Supp.QKDN-mla and Y.QKDN-SDNC)
- Liaisons to all related groups for cooperation
  - ITU-T SG2, SG11, SG17 and ETSI ISG-QKD, ISO/IEC JTC1/SC27

QKD related documents in SG13



Q16/13
(Knowledge-centric trustworthy networking and services)

Y.3800
Overview on networks supporting QKD

Y.3801 (QKDN - Functional requirements)
Y.3802 (QKDN - Functional architecture)

Y.3803
QKDN - Key management

Y.3804
QKDN - Control and management

Y.Supp.QKDN-mla,
Y.QKDN_frint

Y.QKDN_BM
QKDN - Business models

Y.QKDN_SDNC
QKDN - Software defined network control

Q6/13
(Quality of service (QoS) aspects including IMT-2020 networks)

Y.QKDN-qos-gen
General aspects of QoS for QKDN

Y.QKDN-qos-req
Requirements of QoS Assurance for QKDN

Y.3800 - “Overview on networks supporting quantum key distribution”

This Recommendation specifies an overview on networks to support quantum key distribution (QKD) to address network aspects to implement QKD technologies. In particular, this Recommendation addresses the followings:

- an overview of QKD technologies;
- network capabilities to support QKD;
- Conceptual structure and basic functions of QKD networks (QKDN).

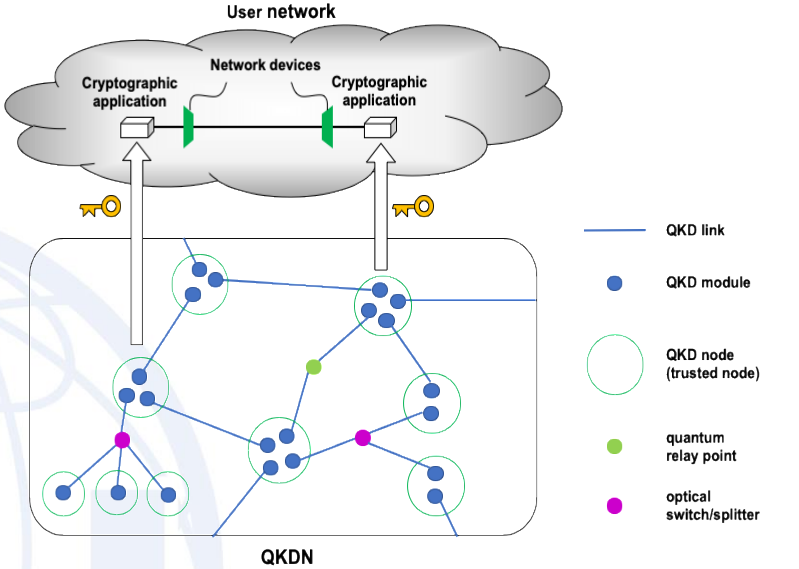


Illustration of QKDN concepts and their relation to a user network

QKDN design considerations:

- Security, scalability, stability, efficiency, application-oriented, robustness, integratability, interoperability, migratability, manageability

Basic functions of QKDN:

- Quantum key generation;
- Key management;
- QKDN control;
- QKDN management.

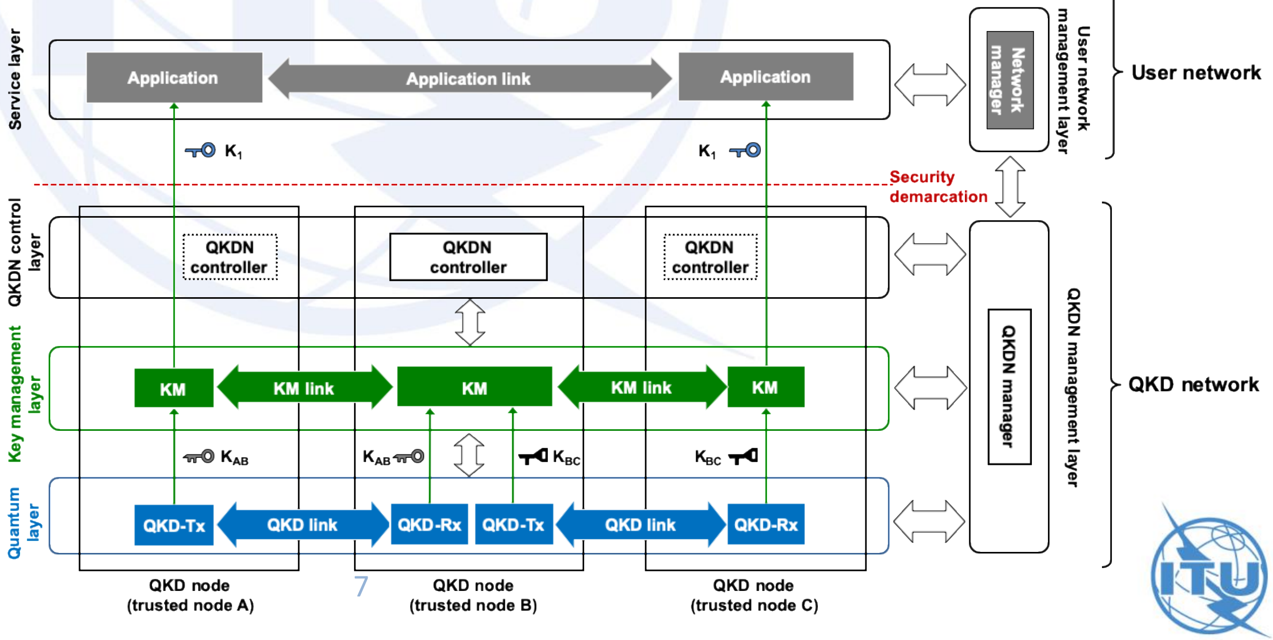


Illustration of the conceptual structures of a QKDN and a user network

Y.3801 - “QKDN - Functional Requirements”

This Recommendation is to specify functional requirements for Quantum Key Distribution network:

- Functional requirements for capabilities of quantum/key management/QKDN control and management layers and other capabilities for QKDN

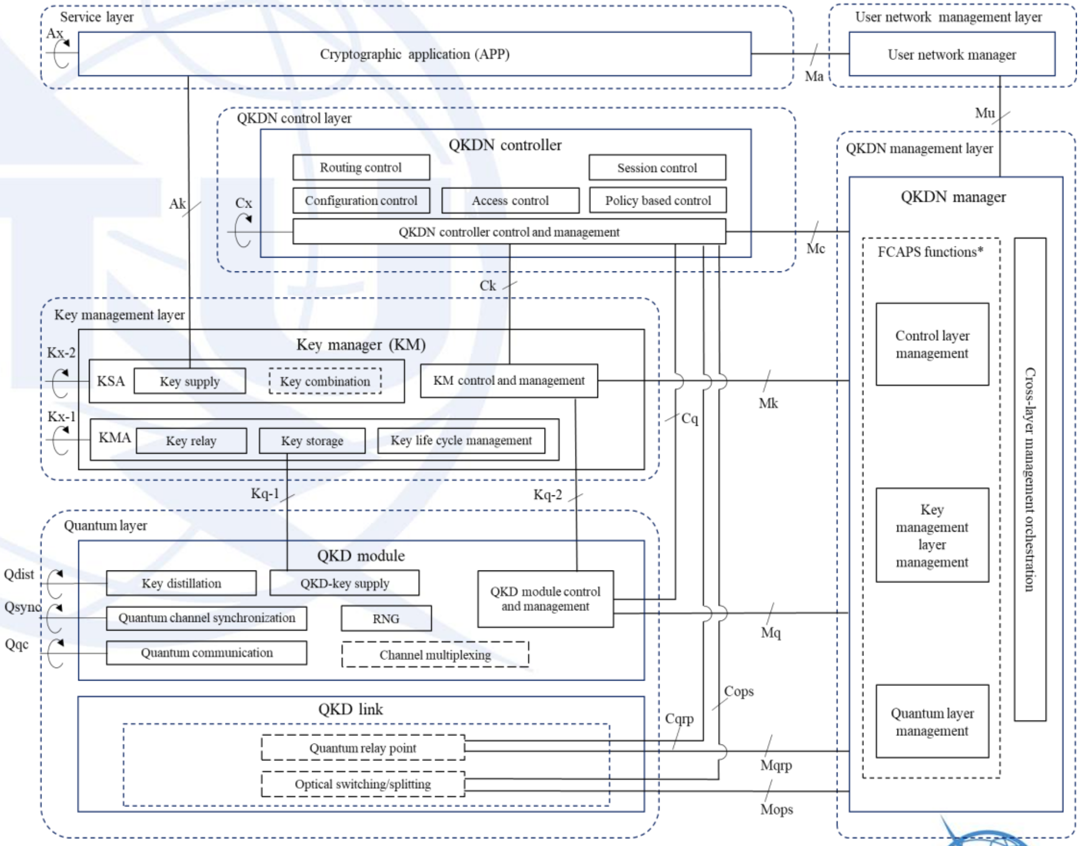
Y.3802 - “QKDN - Functional Architecture”

This Recommendation specifies functional architectures of the Quantum Key Distribution (QKD) network.

In particular, the scope of this draft Recommendation includes:

- **Functional architecture model**
- **Functional elements and reference points**
- **Architectural configurations**
- **Overall operational procedures**

NOTE – This Recommendation addresses the architecture of the QKD network based on the general structure defined in Recommendation ITU-T Y.3800 as a foundation for further QKD network studies.



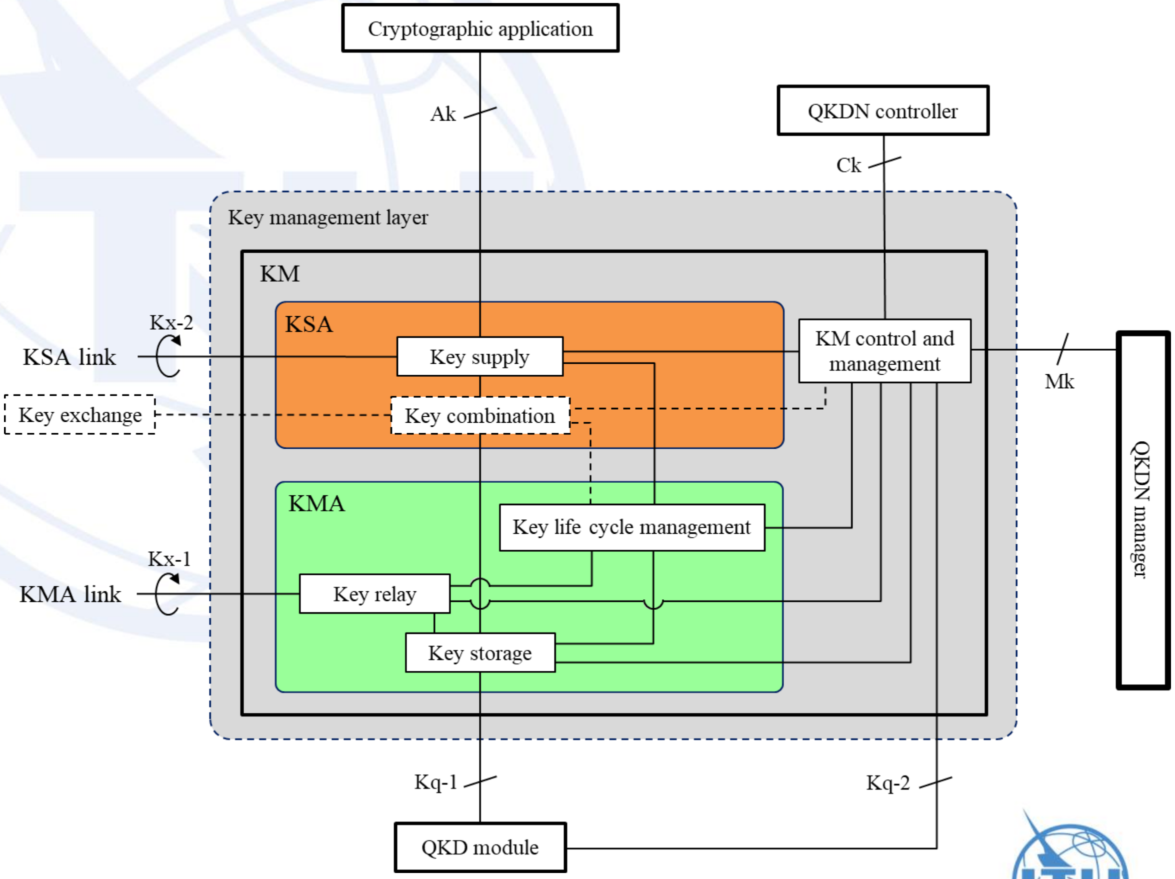
Functional architecture model of QKDN

Y.3803 - "QKDN - Key management"

This Recommendation describes key management for Quantum Key Distribution (QKD) network which addresses technical specifications to help the implementation and operation. In particular, the scope of this draft Recommendation includes:

- **Requirements of key management**
- **Functional elements of key management**
- **Procedures of key management**
- **Key formats (key data and meta-data)**

NOTE – This document refers the overall structure and basic architecture of QKD network which are defined in the Recommendation ITU-T Y.3800.



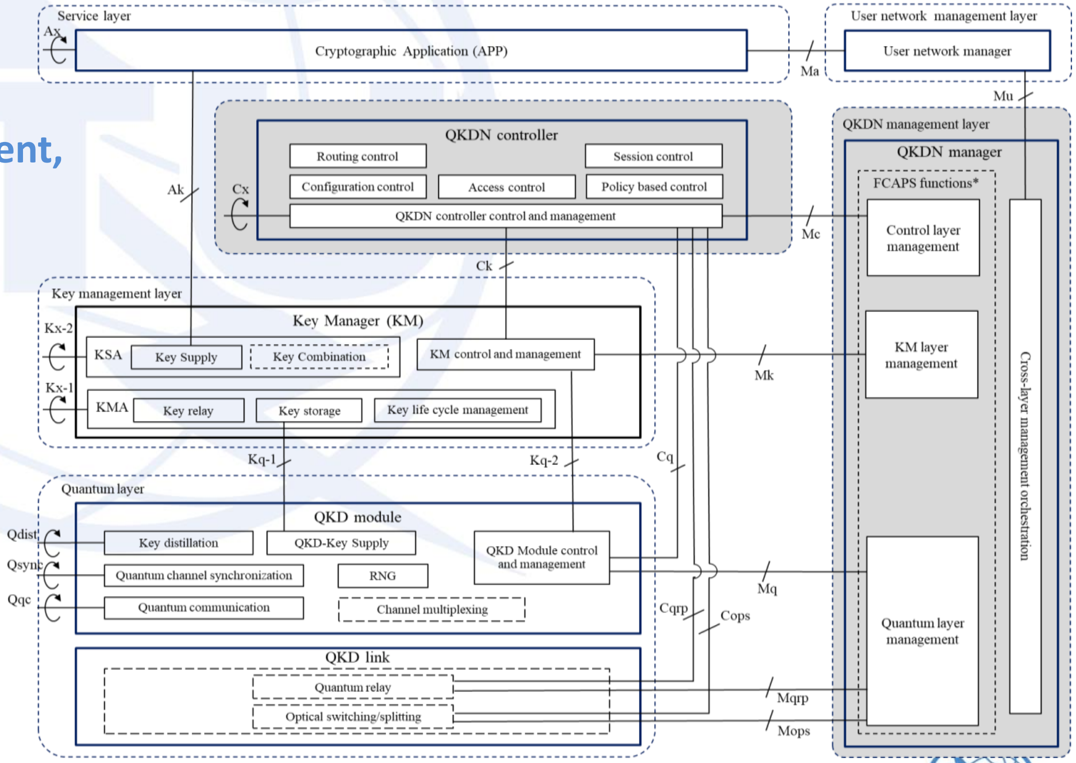
Functional elements and procedure of key management

Y.3804 - “QKDN - Control and management”

This Recommendation is to specify the control, management, and orchestration for Quantum Key Distribution network. This recommendation covers:

- **Functional requirements of QKDN control, management, and orchestration**
- **Functional architecture 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**
- **Appendix: Implementation use cases of QKDN control, management, and orchestration**

Note - Traditional FCAPS functionality which is not specific to QKDN is out of scope of this Recommendation. If necessary, the document will, instead, reference the existing works appropriately.



QKDN control and management high-level functional architecture

Y.QKDN_SDNC - “QKDN - Software Defined Network Control”

This Recommendation specifies the QKDN control functions with the concepts of software defined networks (SDN). The scope of this recommendation includes the following:

- General concepts for introducing SDN into QKDN
- Function requirements of SDN control for QKDN
- SDN-based control architecture for QKDN
- Hierarchical SDN controller for multi-domain QKDN
- Procedures of SDN control functions
- Applications scenarios for SDN controlled QKDN
- Security considerations

Y.QKDN_BM - “QKDN - Business role-based models”

This draft Recommendation describes business roles, business role-based models, and service scenarios in Quantum Key Distribution Network (QKDN) from different deployment and operation perspectives. Especially, this draft Recommendation identifies various business models that require secure communications with QKDN and existing user networks as follows:

- general QKDN applications;
- financial sector;
- healthcare sector;
- transportation sector;
- etc.

This draft Recommendation can be used as a guideline for design of service scenarios that utilize QKDN from business point of views as well as for deployment and operation of QKDN from telecom operators’ point of views.

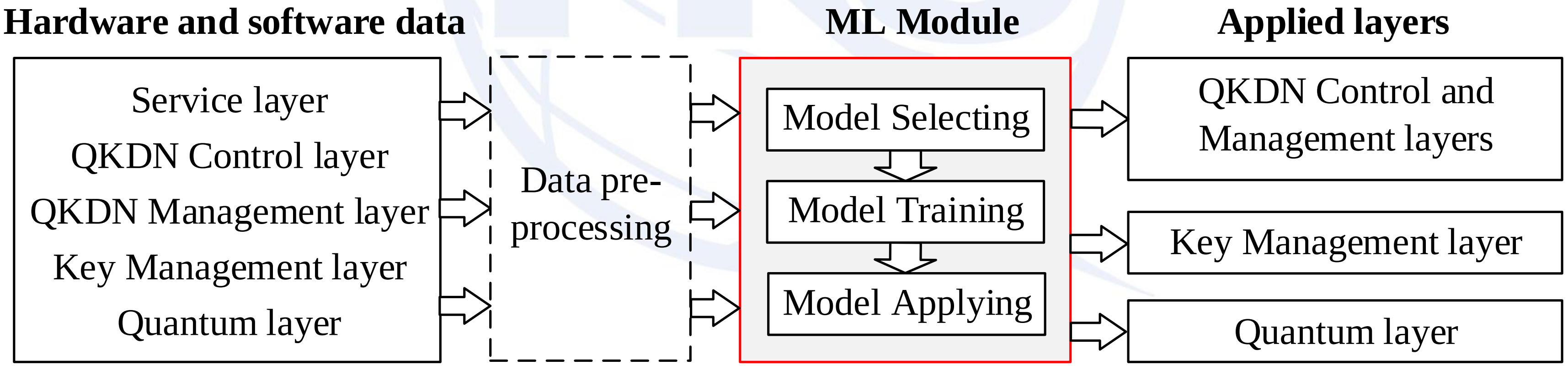
NOTE – This draft Recommendation does not identify, in an exhaustive manner, all business roles, business role-based models, and service scenarios of QKDN.

Y.supp.QKDN-mla - “QKDN – Machine Learning Applications”

This Supplement studies the applications of machine learning (ML) in quantum key distribution networks (QKDNs).

In particular, the scope of this draft Supplement will include:

- Overview of ML applications in QKDN;
- Applications of ML in QKDN at the quantum layer of QKDN;
- Applications of ML in QKDN at the key management layer of QKDN;
- Applications of ML in QKDN at the control and management layers of QKDN.



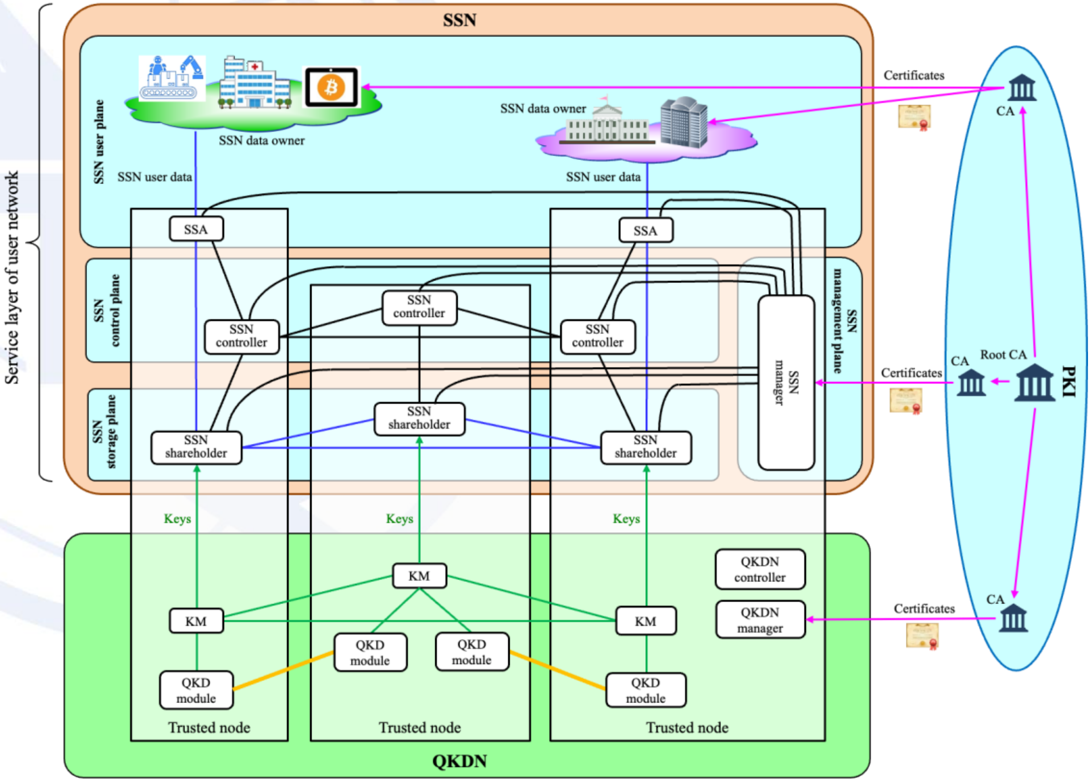
ML module in QKDN

Y.QKDN-frint - “Framework for integration of QKDN and secure storage network”

This Recommendation describes framework for integrating QKDN and secure storage network (SSN)with conventional and emerging secure network infrastructures.

In particular, the scope of this Recommendation includes:

- overview of secure storage network (SSN);
- functional requirements for SSN;
- functional architecture model of SSN;
- reference points;
- operational procedures;
- phase-in scenarios.



A conceptual view of integration of the QKDN with PKI and the SSN

Future plan – this year

- Finalize the development of core QKD related draft Recommendations
  - Y.Supp.QKDN-mla, Y.QKDN-SDNC, Y.QKDN-BM and Y.QKDN_frint: by this year
- Invite new work items on QKD
  - AI for QKDN, time synchronization, interworking
- Close collaboration with related groups
  - Organize a co-located RGM with SG17 Questions
  - Organize a joint workshop with ITU-T and ETSI

Future plan – next study period

- QKDN
  - QKDN core recommendations
- QENS (Quantum Enhanced Networks and services)
  - FG-QIT4N's results
  - QEN supporting technology
  - User networks and related applications

ITU