Ninth SG13 Regional Workshop for Africa on "Standardization of Future Networks and Emerging Network Technologies: African perspectives"

(Abidjan, Côte d'Ivoire, 19-20 September 2023)

Standardization for Quantum Key Distribution Networks in ITU-T SG13

19 September 2023

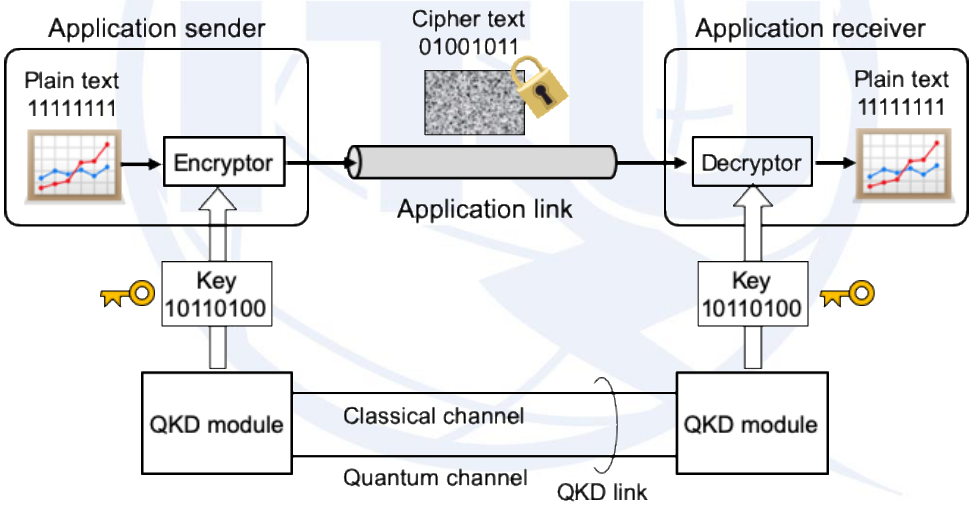
Gyu Myoung Lee

WP3/13 co-chair, Q16/13 Rapporteur

gmlee@kaist.ac.kr

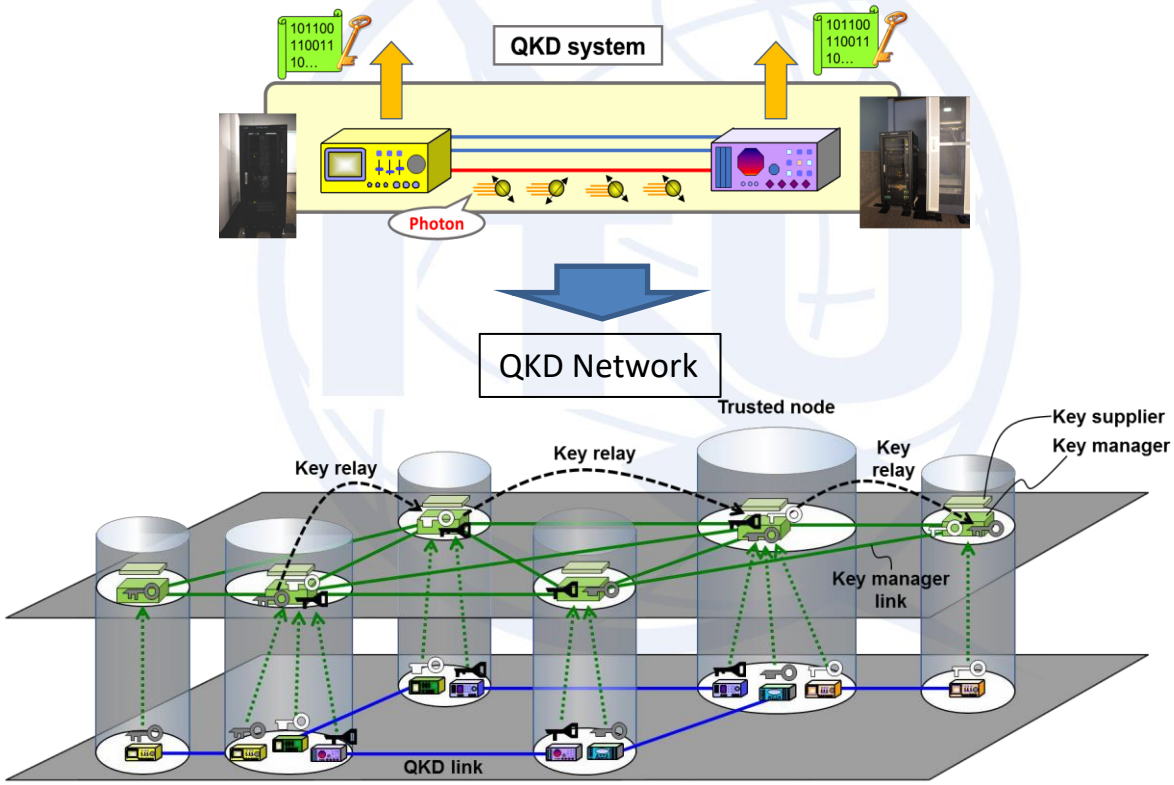
Quantum Key Distribution (QKD)

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

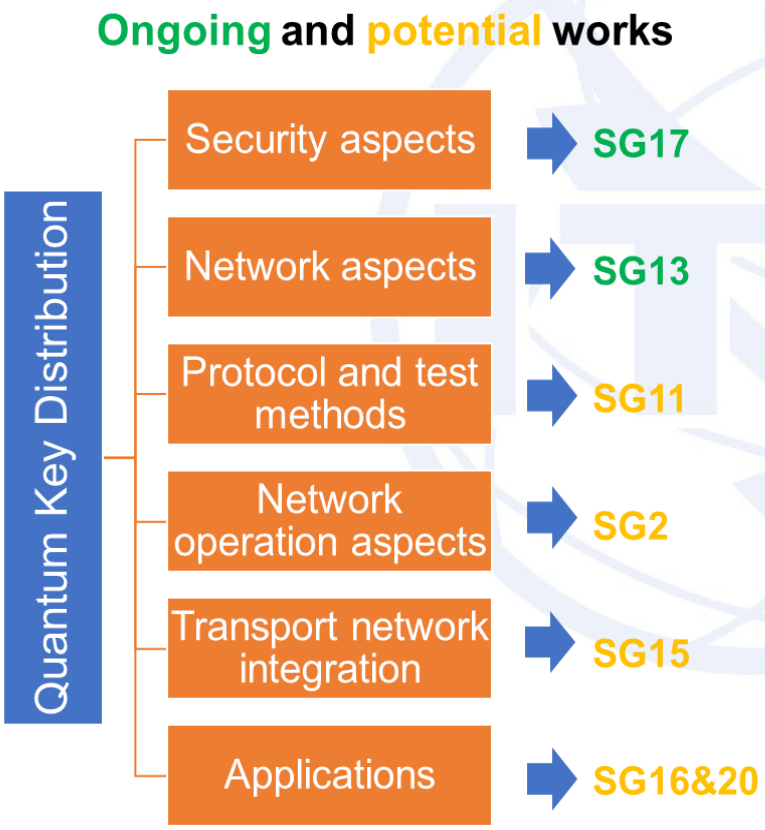


Configuration example of QKD use for securing a P-to-P application link

From QKD system to QKD network

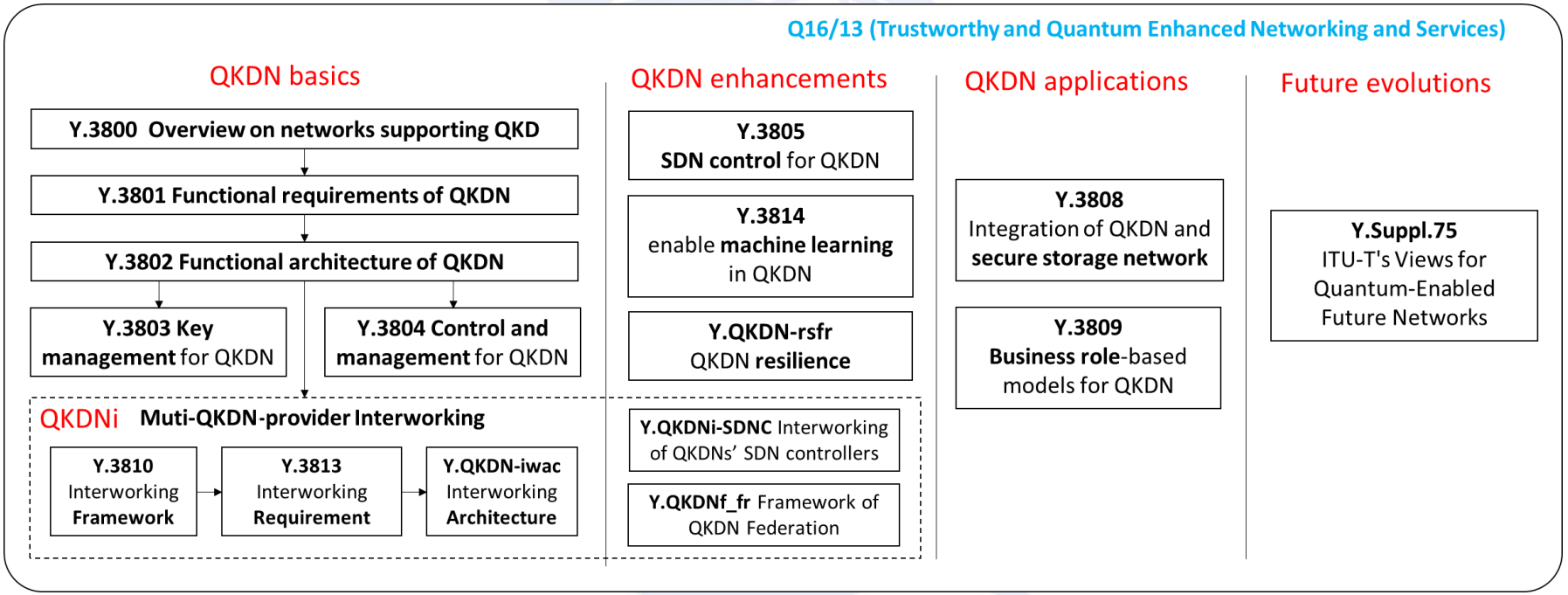


QKDN standardization aspects in the context of ITU-T



- July 2018
  - First initiative on QKDN – Y.QKDN_FR
- SG13 has published 15 Recommendations and 1 supplement on QKDN

QKD related documents in Q16/13

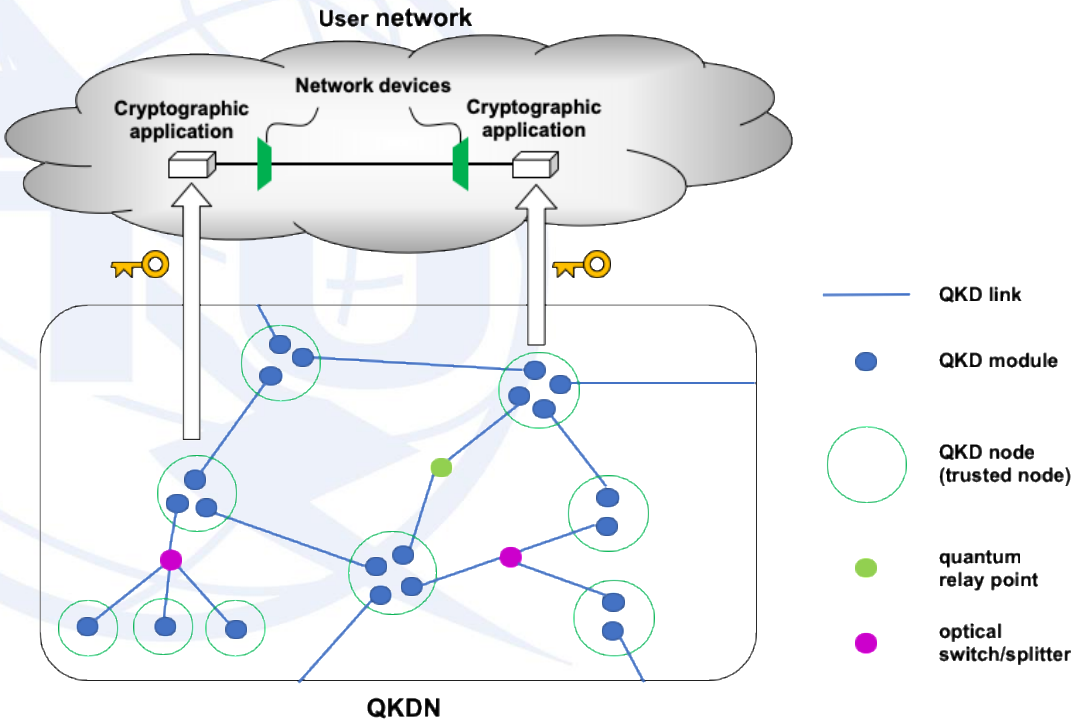


TR.QN-UC: Use cases of quantum networks beyond QKDN, **Y.supp.QKDN-UC**: Use cases of QKDN
Y.QKDN-rsrq: Requirements for resilience, **Y.QKDN-TSNfr**: Integration of QKDN and time-sensitive network
TR.QKDN-nq: Integration of quantum key distribution network with non-quantum cryptographies

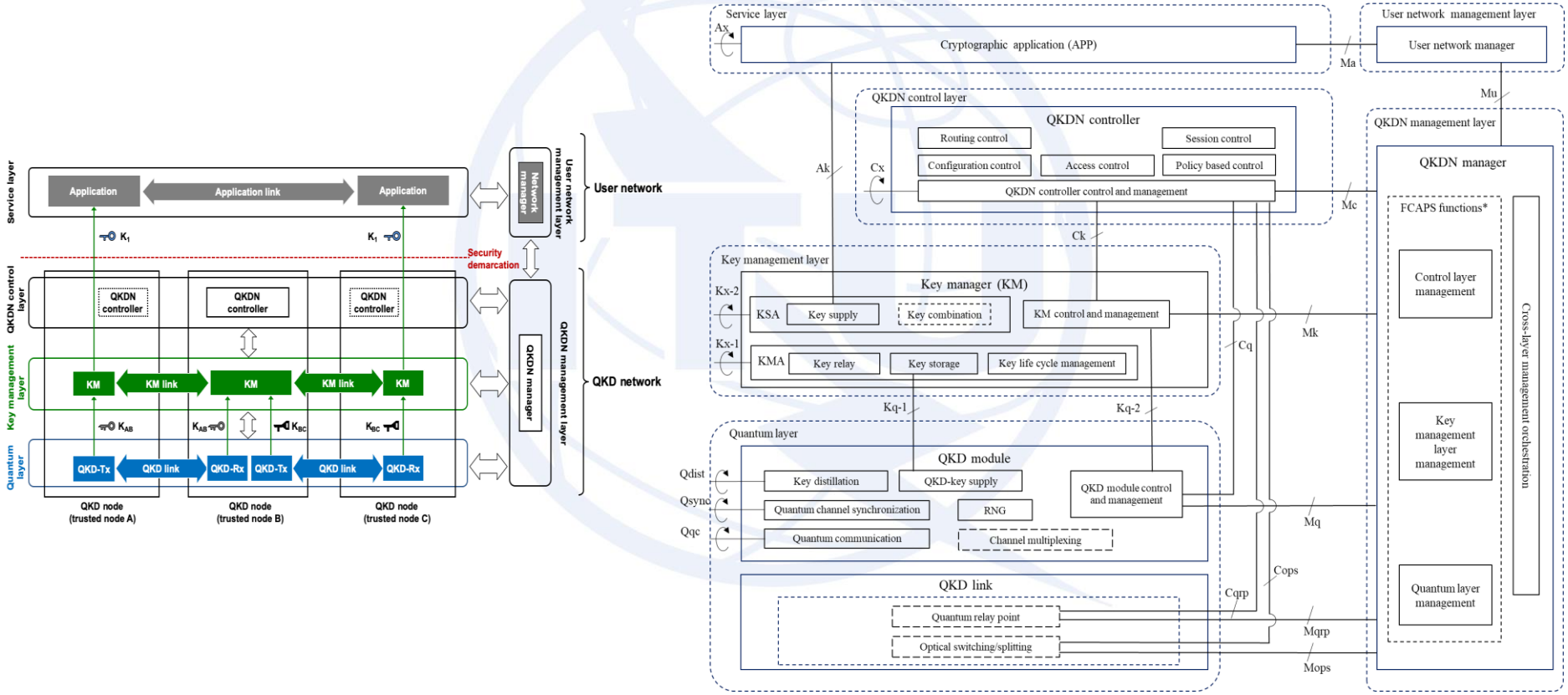
QKDN concepts and their relation to a user network

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

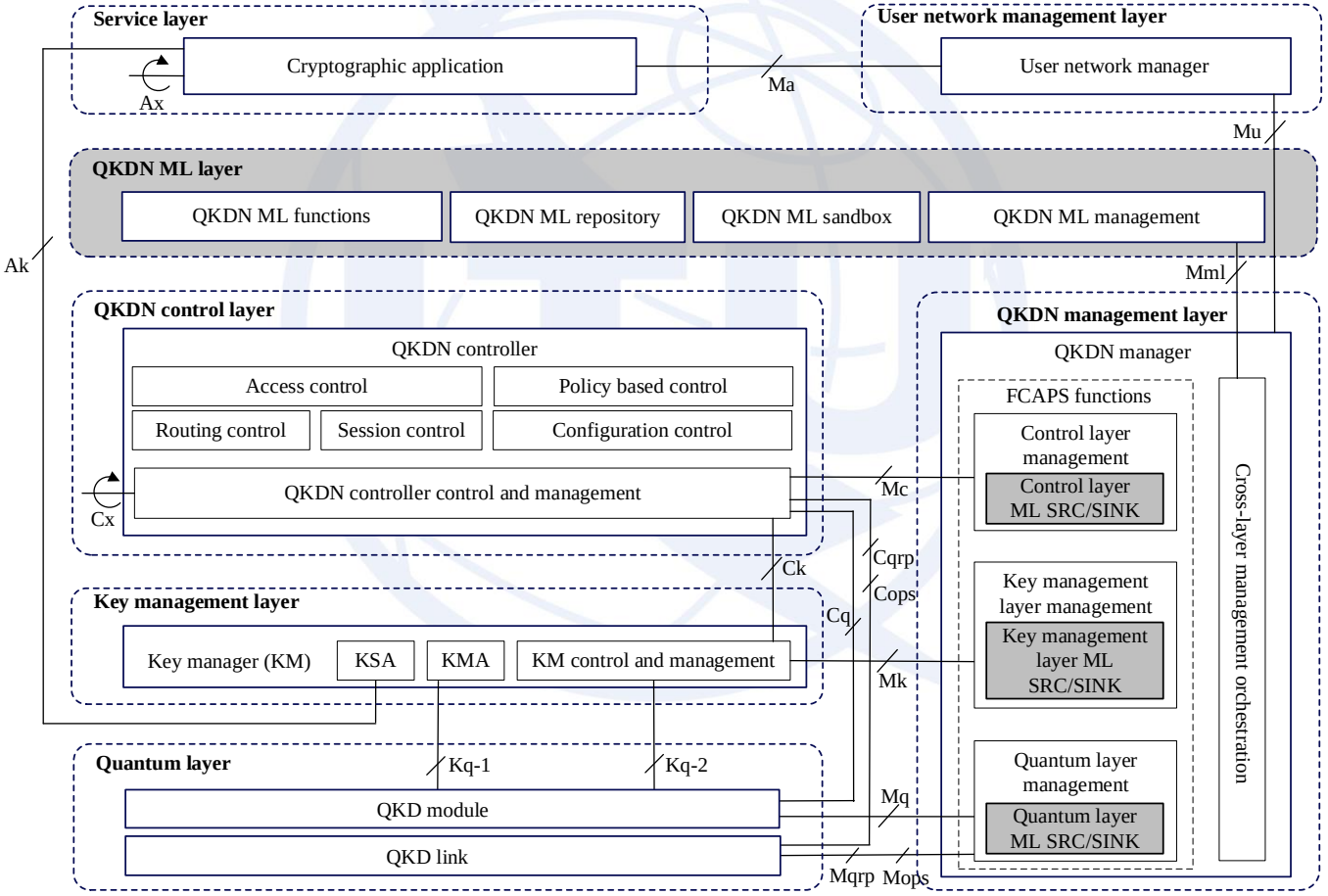
Y.3800 - "Overview on networks supporting quantum key distribution"



QKDN architecture

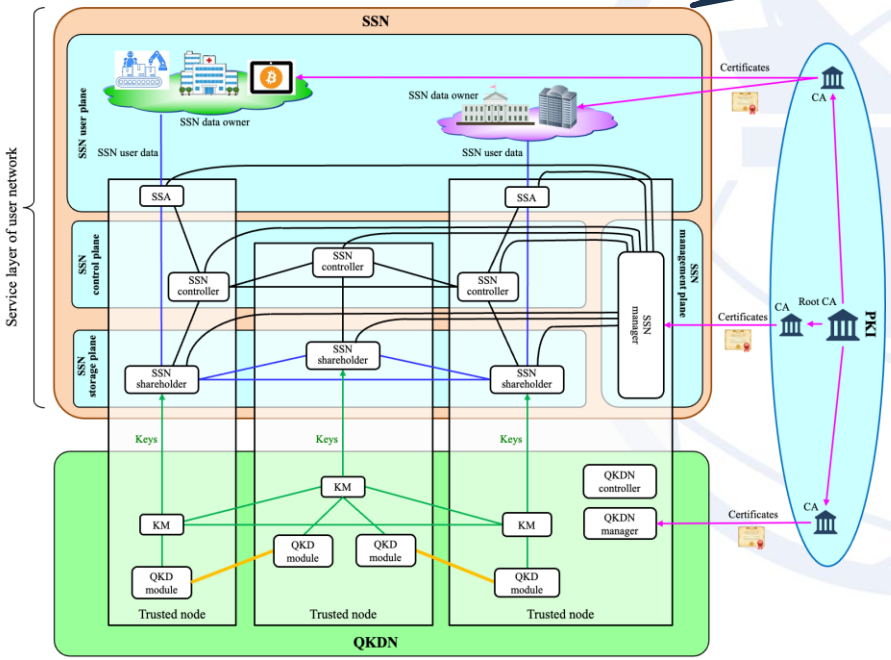


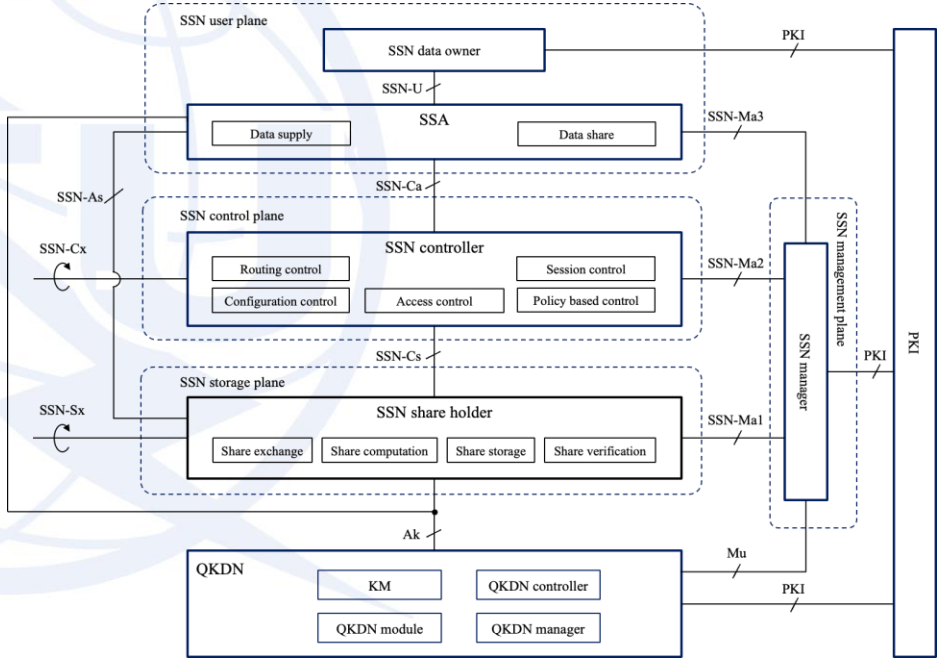
Machine Learning (ML) enablement



Integration of QKDN and secure storage network

Support of multiple encryption methods, such as QKD-OTP or QKD-AES hybrid (key generation rate vs data size)



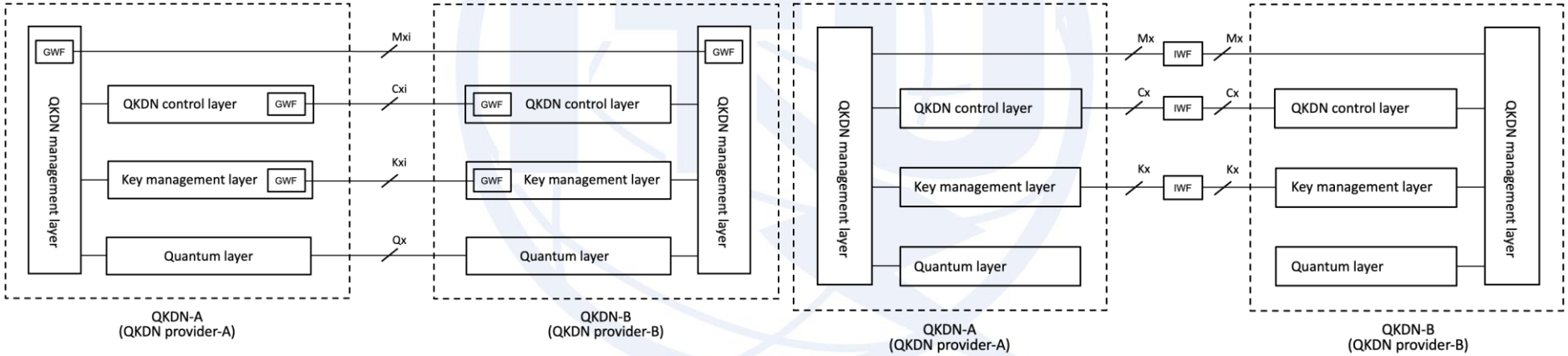


Optimal key supply control by user data size

QKDN interworking (QKDNi)

QKDNi with GWFs

QKDNi with IWFs



Recent progress (Geneva, 13-24 March 2023)

- **2 supplements agreed**
  - Supplement 75 (formerly TR-QEFN), Quantum key distribution networks – Quantum-Enabled Future Networks
  - Supplement 74 (formerly Y.supp.QKDN-roadmap), Standardization roadmap on Quantum Key Distribution Networks

- **4 new work items**
  - TR.QNDN-nq, Overview for integration of quantum key distribution network with non-quantum cryptographies
  - Y.supp.QKDN-sync, Analysis of Time Synchronization in Quantum Key Distribution Networks
  - Y.QKDN-TSNfr, Framework for integration of quantum key distribution network and time-sensitive network
  - Y.QKDN-rsrq, Requirements for quantum key distribution network resilience

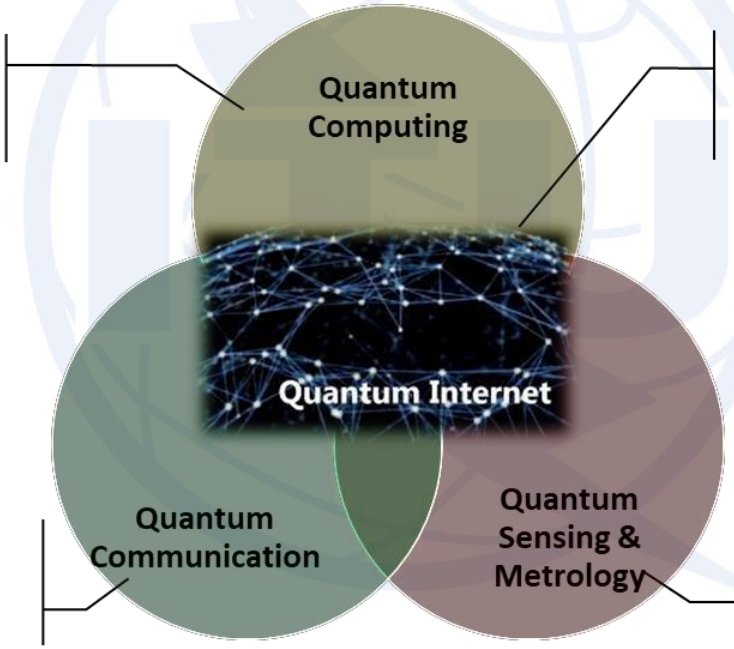
Recent progress (Geneva, 26 July 2023)

- **2 Recommendations consented**
  - Y.3818 (formerly Y.QKDN-iwac), Quantum key distribution networks interworking – architecture
  - Y.3815 (formerly, Y.QKDN-rsfr), Quantum key distribution networks – overview of resilience

- **Others**
  - Discussion on “Overview of Quantum Network”
  - Amendments to ITU-T Y.3802, Y.3803, Y.3804, Y.3805, Y.3811 and Y.3814

Quantum Information Technologies (QIT)

Crack classical crypto.,
Power up signal processing
and data analysis
……



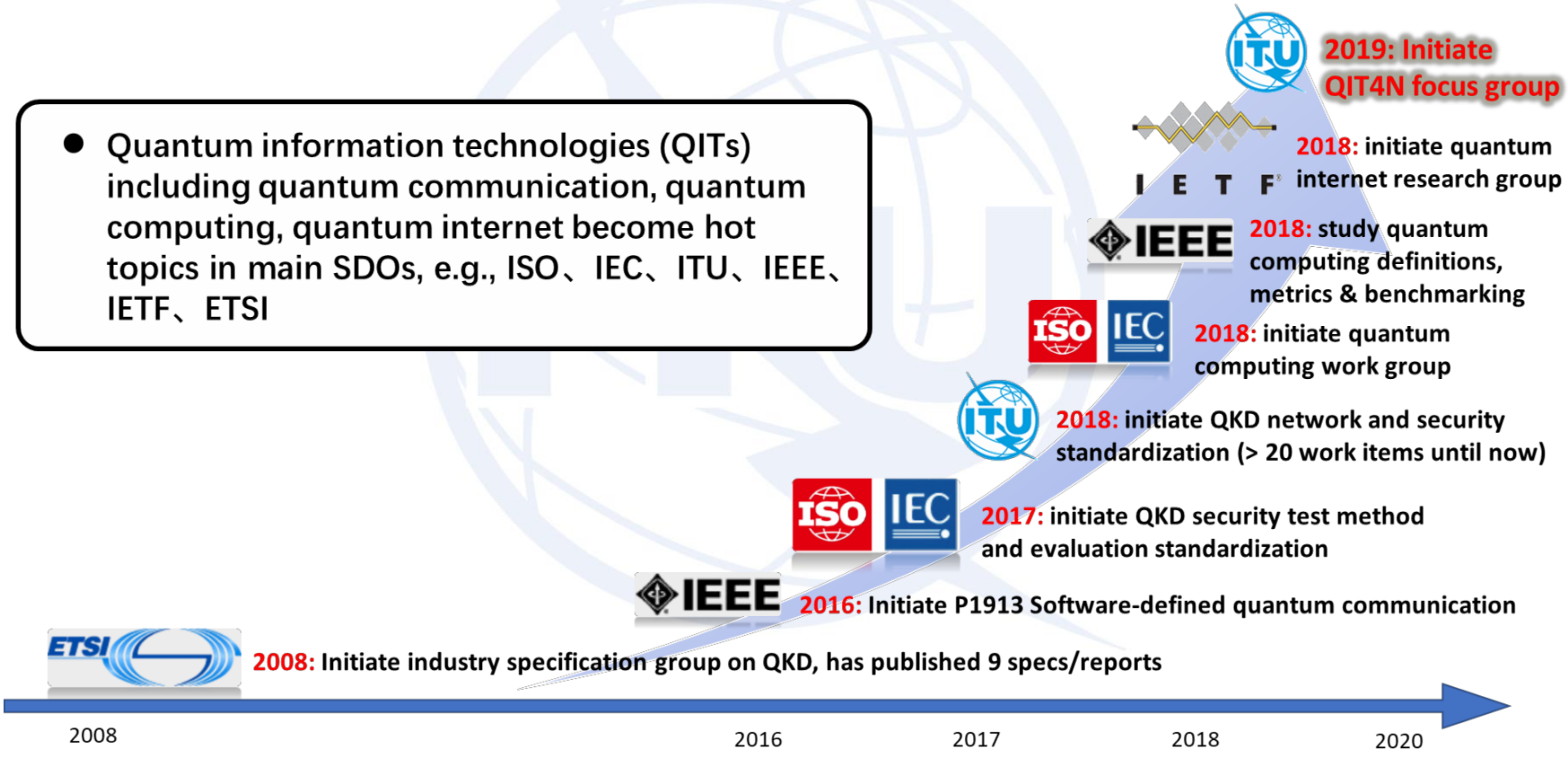
New applications, e.g.,
distributed quantum computing,
quantum sensor network,
world clock,
……

Eavesdropping immune,
Long term security,
Quantum info. transmission

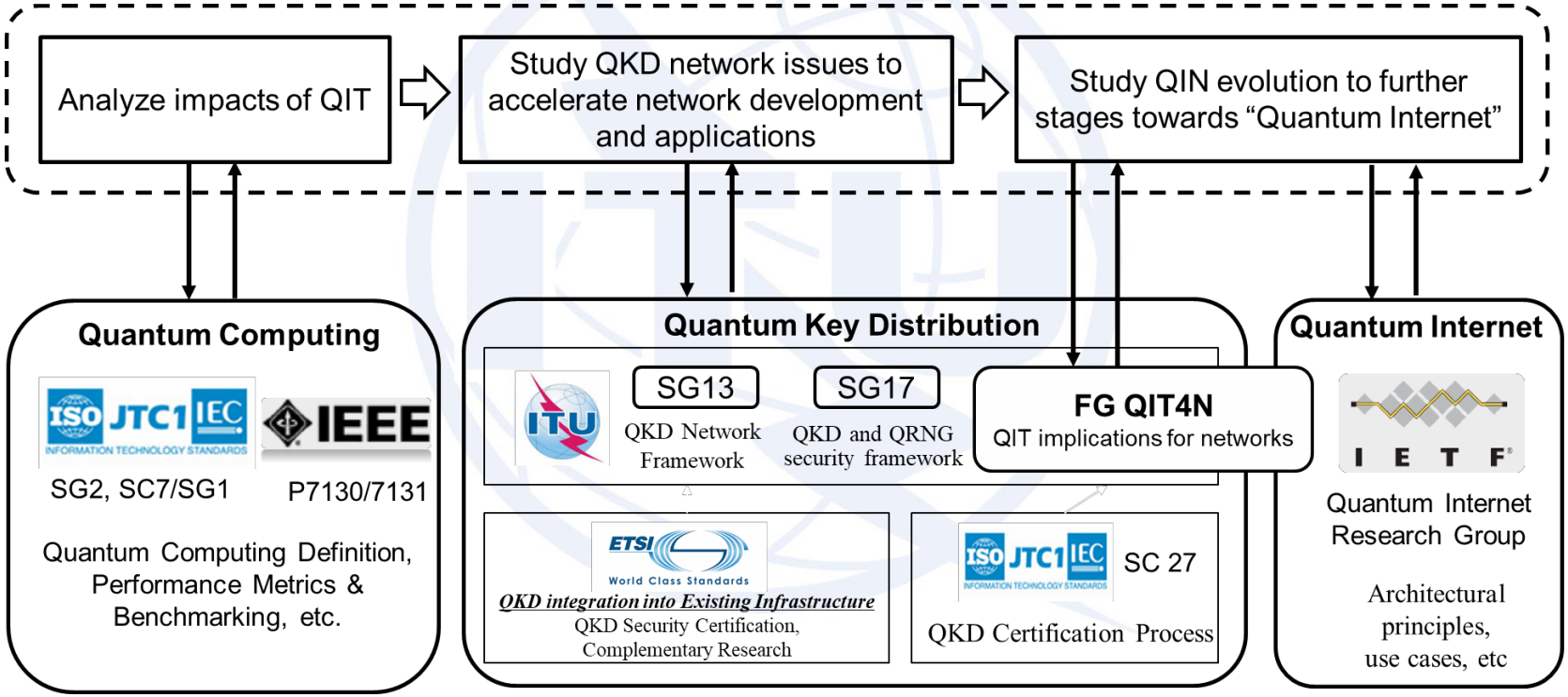
High precision measurement
to enhance positioning,
navigation, timing, sensing,

A Landscape of QIT Standardization Activities (1/2)

- Quantum information technologies (QITs) including quantum communication, quantum computing, quantum internet become hot topics in main SDOs, e.g., ISO、IEC、ITU、IEEE、IETF、ETSI

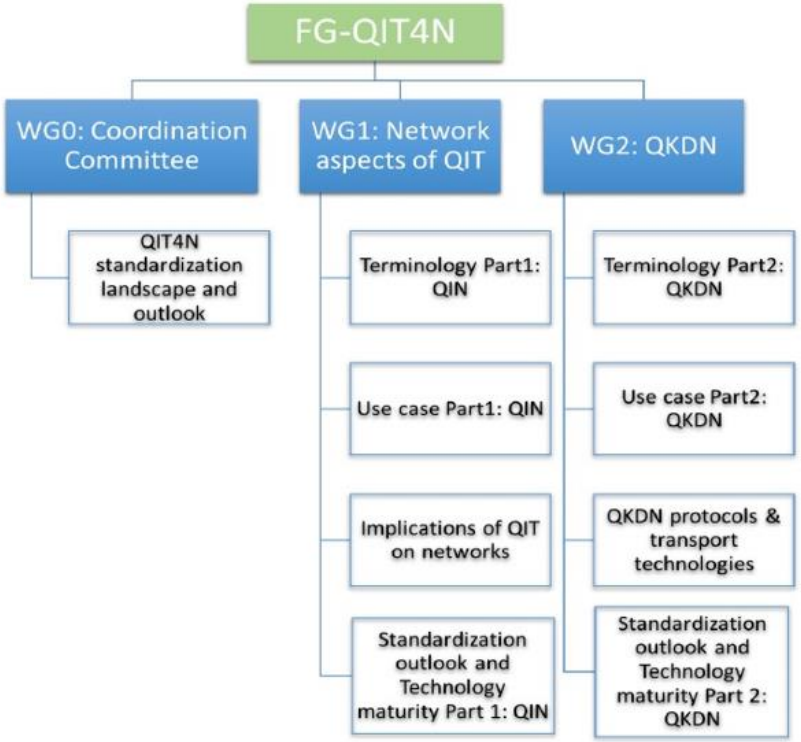


A Landscape of QIT Standardization Activities (2/2)



FG-QIT4N

- Considering evolution and applications of QIT for networks
  - Telecom/network aspects of QKD networks
  - QIN technology and network evolution
- The FG outputs focus on terminology and use cases
- To provide necessary technical background information and collaborative conditions
- To provide an open cooperation platform with ITU-T study groups and other SDOs



Future plan – next study period

- QKDN
  - Additional QKDN Recommendations
- QEFN&S (Quantum-Enabled Future Networks and Services)
  - FG-QIT4N's results
  - Supporting technology for QEFN
  - User networks and related applications (Vertical Sectors)

Conclusion

- **Short term – Standardization on QKDN**
  - Scale up from QKD systems to QKD networks
  - Enhancement of available technologies for Key management
  - New technical solutions for control and management in QKDN
  - Interworking issues with multiple providers and/or different technologies
  - ML enablement, Time synchronization, E2E cryptography service, etc.

- **Long term – Standardization on QEFN (or Quantum Networks)**
  - QKD integrated in various networks (5G and beyond)
  - Fundamental quantum mechanics (entanglement, superposition and non-cloning)
  - Support emerging applications with quantum sensing, computing


ITU