National Institute of Information and Communications Technology

ITU Workshop on Quantum Information Technology (QIT) for Networks (Shanghai, China, 5-7 June 2019)

QKD standardization in ITU-T SG13

National Institute of Information and Communications Technology (NICT)
KENYOSHI Kaoru
TAKEOKA Masahiro

Summary

- Q16/13 studies the QKDN (quantum distribution network). Three WIs have been created on this topic.
- The first ITU-T draft Recommendation on QKDN is **Y.QKDN_FR** “Framework for Networks to supporting Quantum Key Distribution”. This document is expected to be consented at the next SG13 meeting in June.

QKDN in ITU-T SG13

- Q16/13 launched a WI Draft Recommendation **Y.QKDN_FR** “Framework for Networks to supporting Quantum Key Distribution” in July 2018. This draft was finalized at the Q16/13 interim meeting in Tokyo, 14-17 May.
- Japanese delegations proposed a new work item on the draft Recommendation **Y.QKDN_KM** “Key management for Quantum Key Distribution Network” at the SG13 meeting in March 2019. This new work item was approved and the initial draft was created.
- During the discussions at the SG13 meeting in March 2019, Q16/13 agreed to split the architecture of QKD network from Y.QKDN_FR and created a separated new work item on the draft Recommendation **Y.QKDN_Arch** ”Functional Architecture of the Quantum Key Distribution Network”.

Y.QKDN_FR

Title: Framework for Networks to supporting Quantum Key Distribution

Scope

This Recommendation describes the framework for Networks to support Quantum Key Distribution (QKD), which addresses architectural network aspects to help the implementation of QKD technologies on user network.

In particular, the scope of this draft Recommendation includes:

- QKD technologies
- Relationship between user network and QKD technologies
- Integrated network
- Network requirements to support QKD technologies and QKD network
- General structure of QKD network
- Basic functions of QKD network
- Overall service procedure in the layered model

Y.QKDN_FR

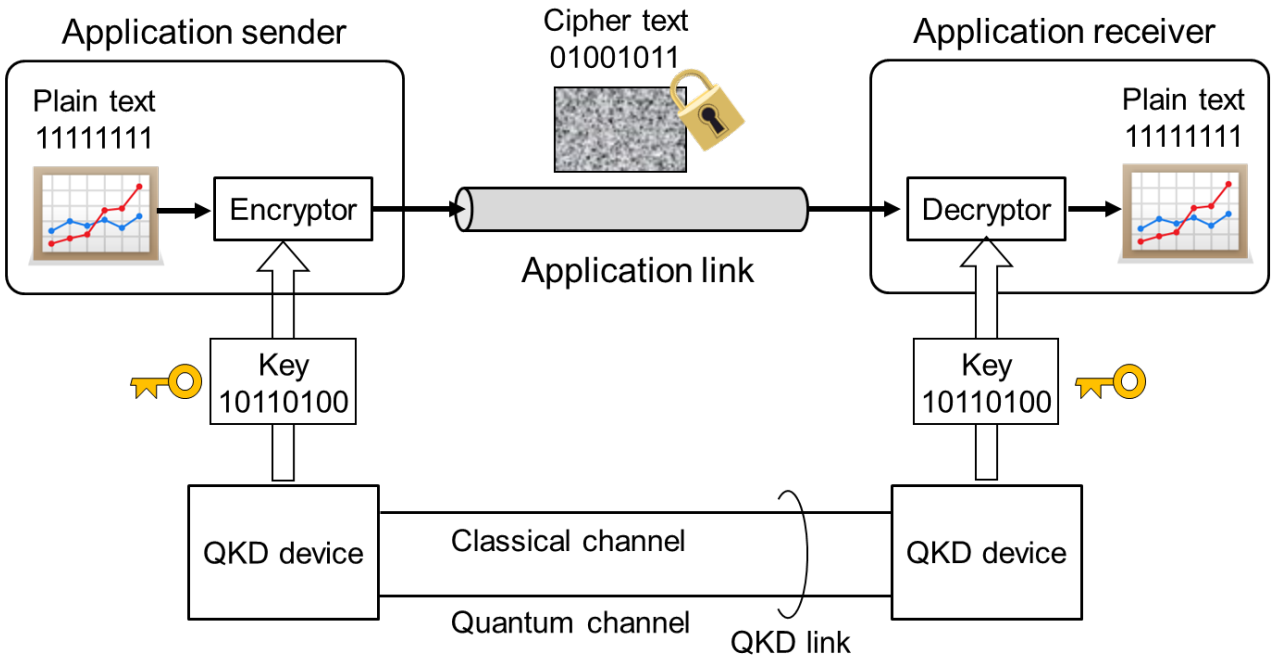

Figure 1. Configuration of QKD application for securing a P-to-P link in a user network.

Y.QKDN_FR

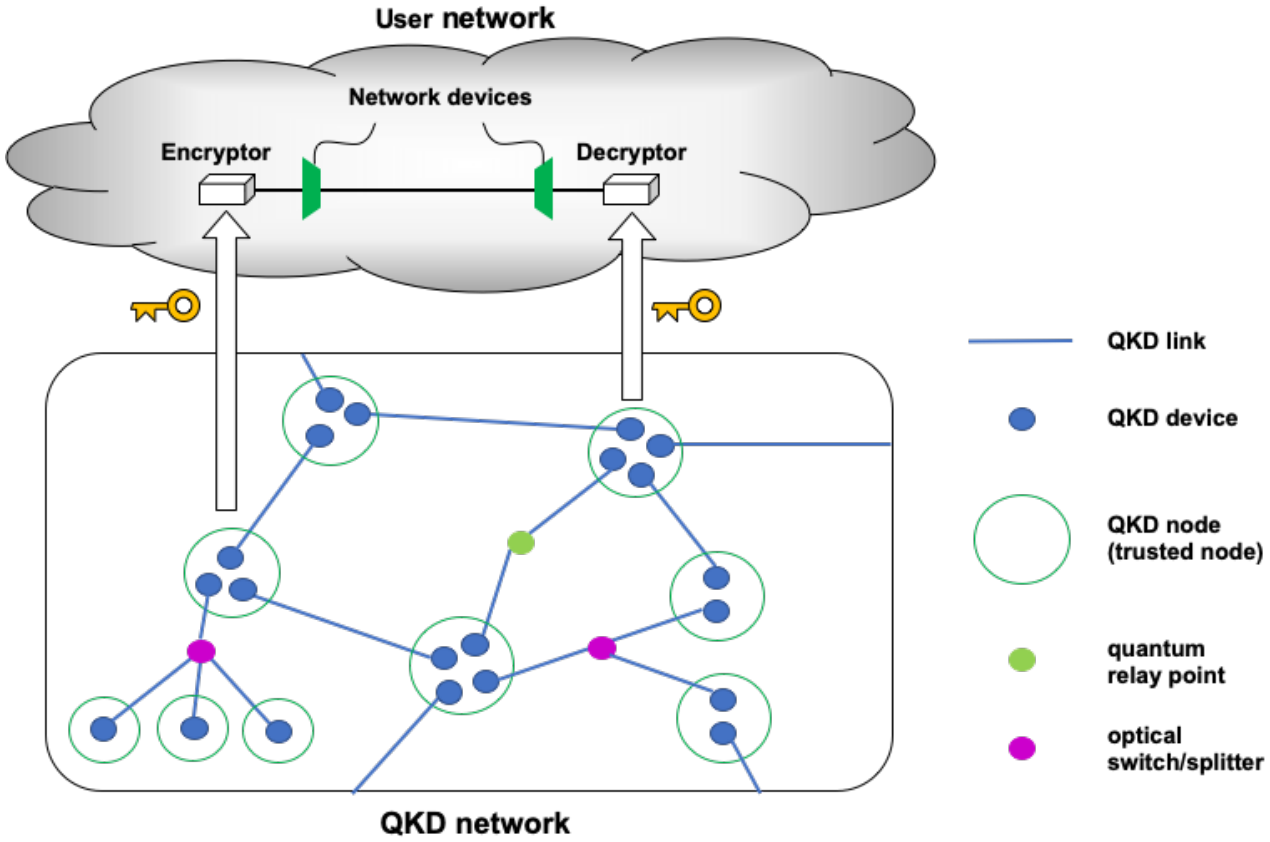

Figure 2. General concept and technologies of QKD network and its relation to user network.

Y.QKDN_FR

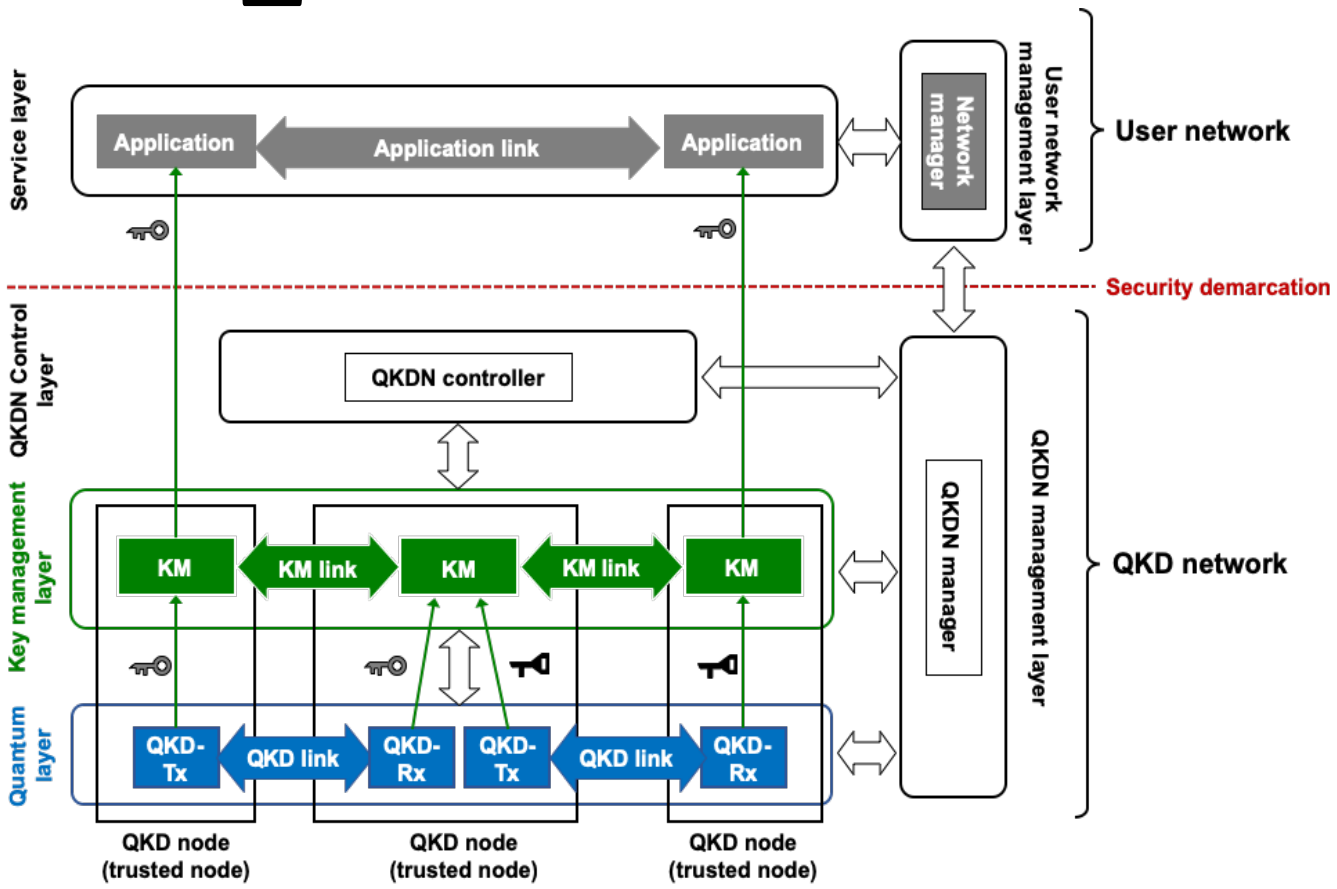

Figure 3. General structure of QKD network, user network, and security demarcation (red dashed line)

Y.QKDN_FR

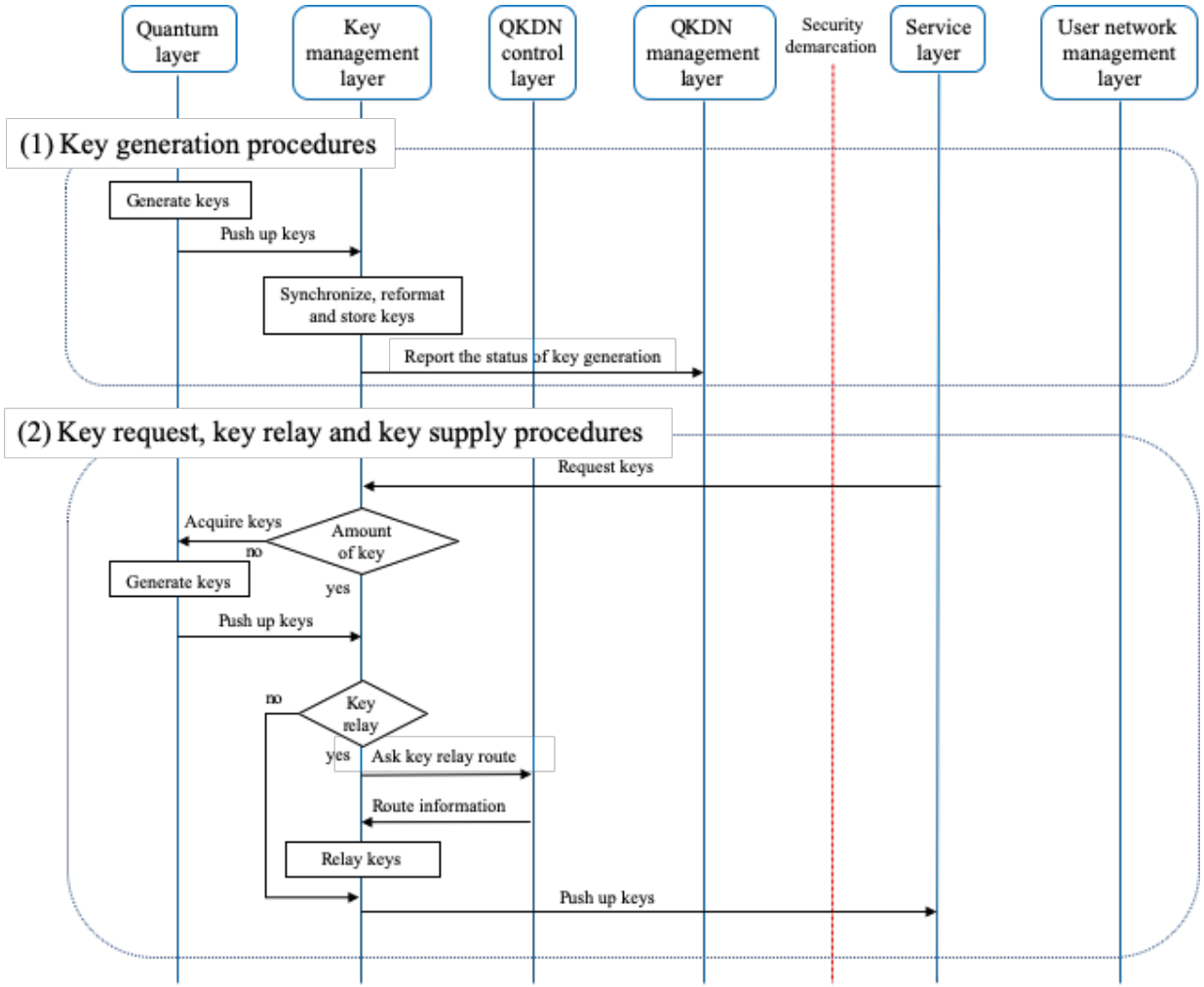

Figure 4.Service procedure among relative layers

This figure is proposal from Japanese contribution at the Q16/13 rapporteur meeting in June

Y.QKDN_Arch

Title: Functional Architecture of the Quantum Key Distribution Network

Scope

This Recommendation provides functional architectures of the Quantum Key Distribution (QKD) network. Following the reference model, the associated functional elements, reference points, a deployment model, operational procedures of the QKD network are then specified.

- In particular, the scope of this draft Recommendation includes:
- The reference model
- Functional elements and reference points
- Deployment model
- Overall operational procedures

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

Y.QKDN_Arch

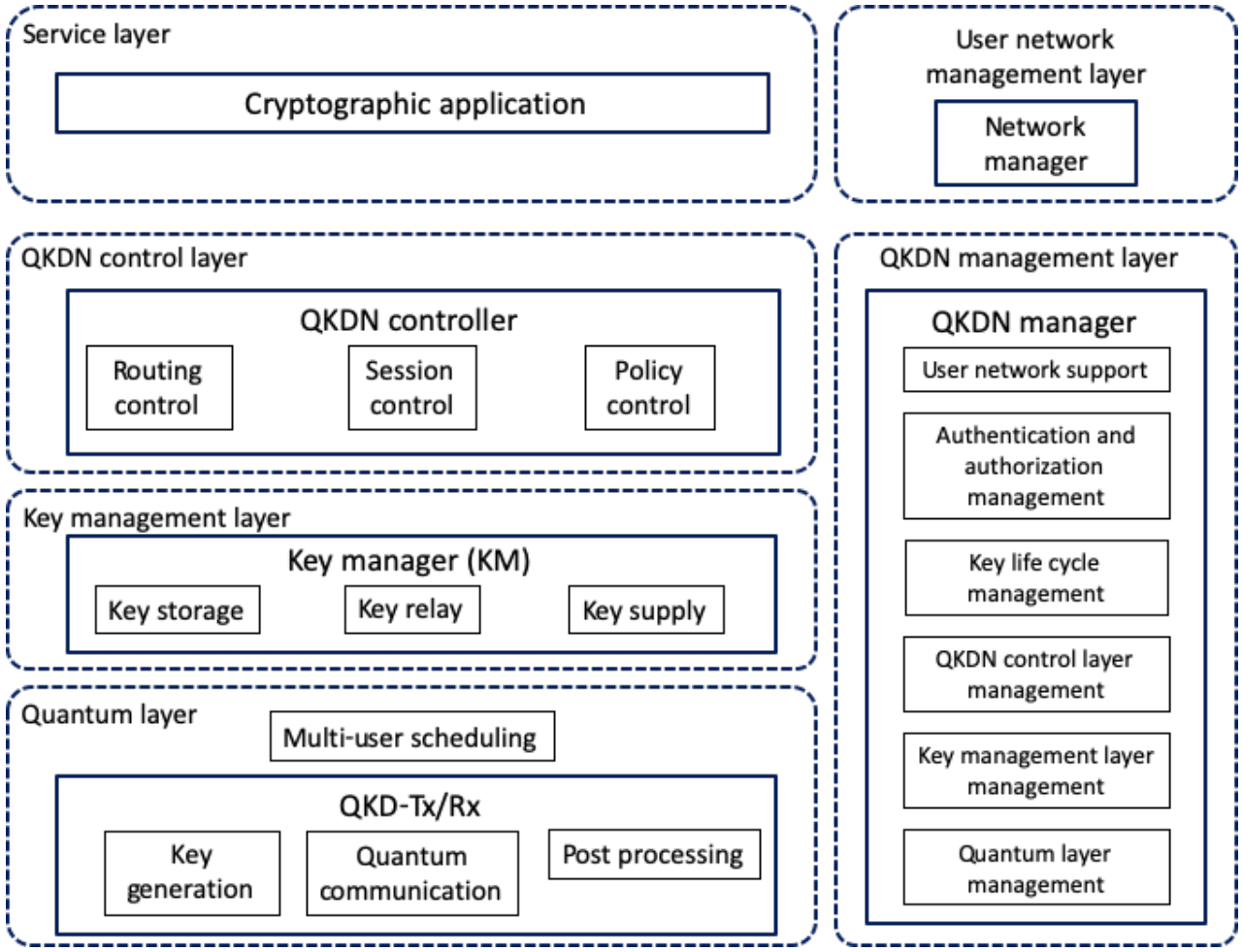

Figure 6.Functional architecture model of QKD network

This figure is proposal from Japanese contribution at the Q16/13 rapporteur meeting in June

Y.QKDN_KM

Title: Key management for Quantum Key Distribution Network

Scope

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)

This document refers the overall structure and basic architecture of QKD network which are defined in the Y.QKDN_FR.

Y.QKDN_KM

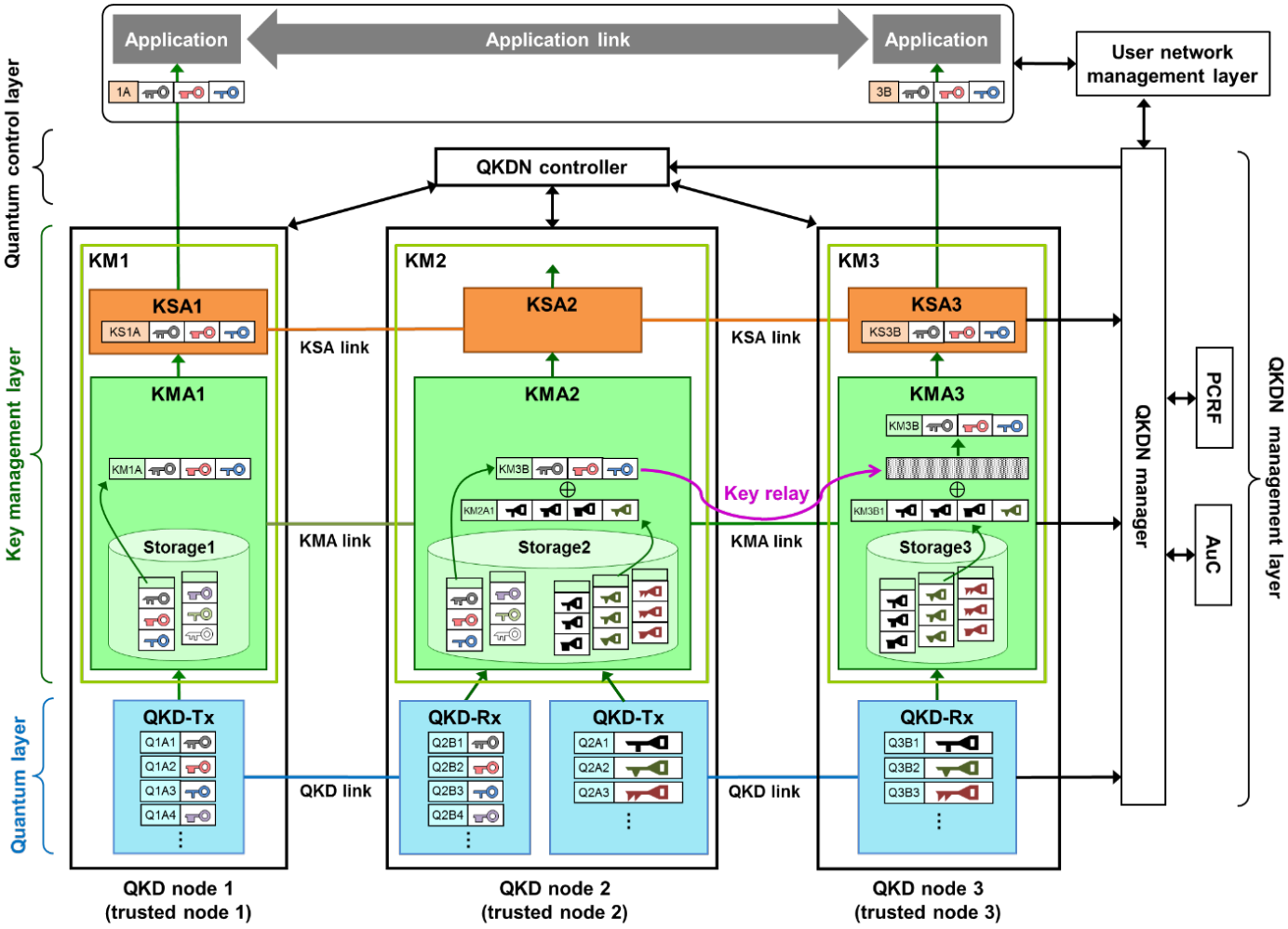

Figure 6.Functional elements and procedures of key management

Q16/13 interim meeting in Tokyo

1. Date and time : 14 – 16 May 2019
2. Venue: NICT (Tokyo, Japan)
3. Participants : 40 delegates (from Japan, China, Korea, UK, Germany, Switzerland)
4. Summary of the results

- Mr. Kenyoshi (NICT) was the acting rapporteur of the meeting.
- 14 contributions were submitted.
- Three draft Recommendations; Y. QKDN_FR, Y. QKDN_KM, Y. QKDN_Arch were discussed and the revised drafts were created.
- The output document of Y.QKDN_FR was carefully reviewed and finalized for consent at the next June SG13 meeting.
- China proposed a new WI on the SD- QKDN "Software defined quantum key distribution network", but it was not discussed, because it was out of the scope of the interim meeting.

Conclusion

- Q16/13 vigorously studies QKD (quantum key distribution). Currently Q16/13 studies three draft Recommendations on this topic.
- Y.QKDN_FR is going to be consented at the next SG13 meeting in June. It will be the first ITU-T Recommendation on quantum.
- The interim meeting in Tokyo in May thrived and successfully concluded. Proposed new work item on SD-QKD will be discussed at the next SG13 meeting.
- Next meeting: SG13 co-located rapporteur group meetings followed by WP meetings (Geneva, 17-28 June 2019)