PEOPLE.
TECHNOLOGY.

QKD with X.509

Hyungsoo (Hans) KIM, KT (hans9@kt.com)

ITU-T SG13 Vice-chair and Working Party 1 Chair

Active standardization on QKD-related

ITU-T SG13, QKD network-related standardization from 2018

*** The mandate of SG13; future networks & emerging technologies**

First Proposal for QKD network ('18.07)

ITU-T SG13

"Rec. Y.QKDN_FR"

First Standard for QKD network ('19.06)

ITU-T SG13

"Rec. Y.3800"

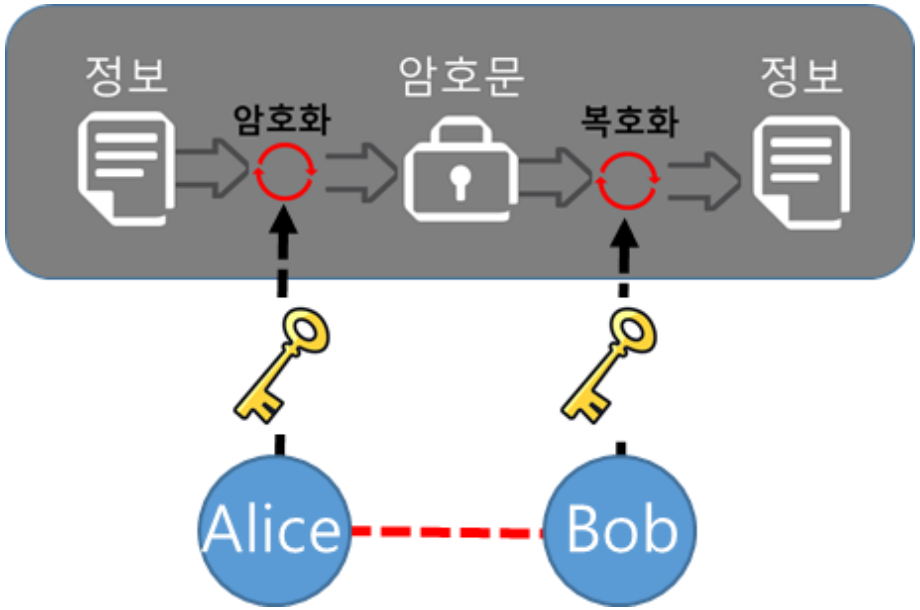
40 more documents are developed ('23.05)

FG QIT4N, SG11, SG17

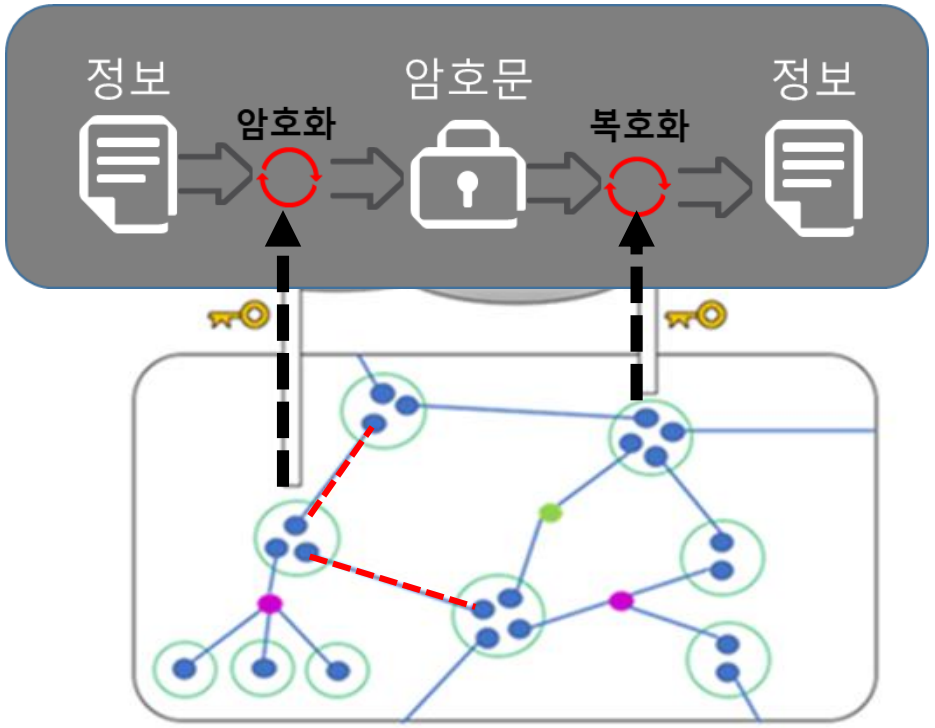
"Interface, Security, etc."

QKD as a network

For cost-effective deployment, operation and maintenance



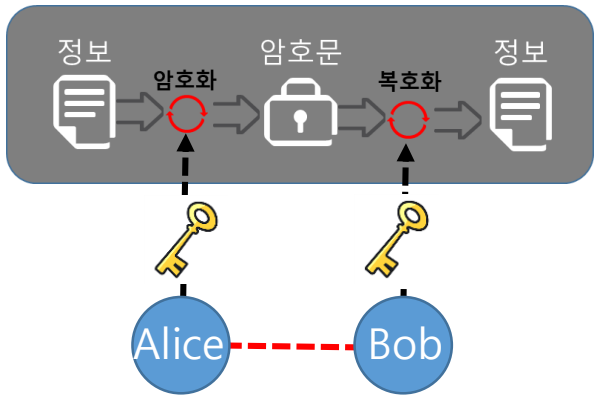
QKD system



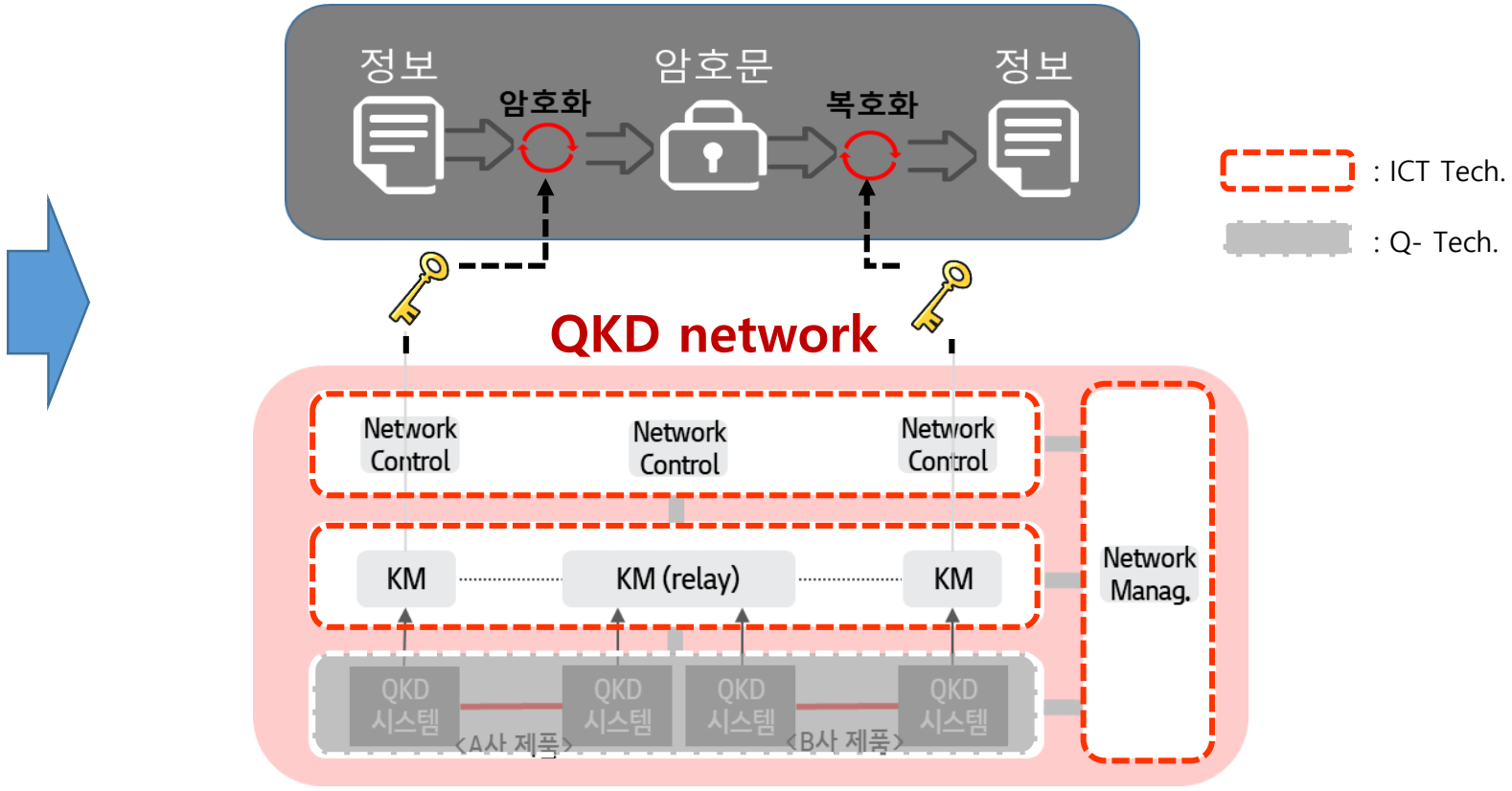
QKD network

Layered model of QKD network in Y.3800

For cost-effective deployment, operation and maintenance



QKD system



<ITU Y.3800>

QKD network implementations (~ ’22.12)

KT, the QKD service provider/network operator on various sectors

<Field Test on Leased-line>

2018

<Field Test on 5G network>

2020

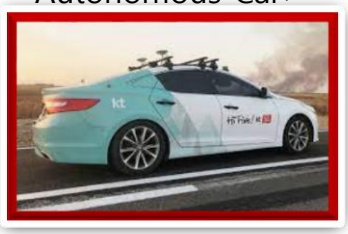
<Implementation on Hyundai Heavy Industry & The Navy Headquarter>

<Implementation on St. Mary’s Medical Centers>

2021

<Quantum-Robot>

<Quantum-Autonomous Car>

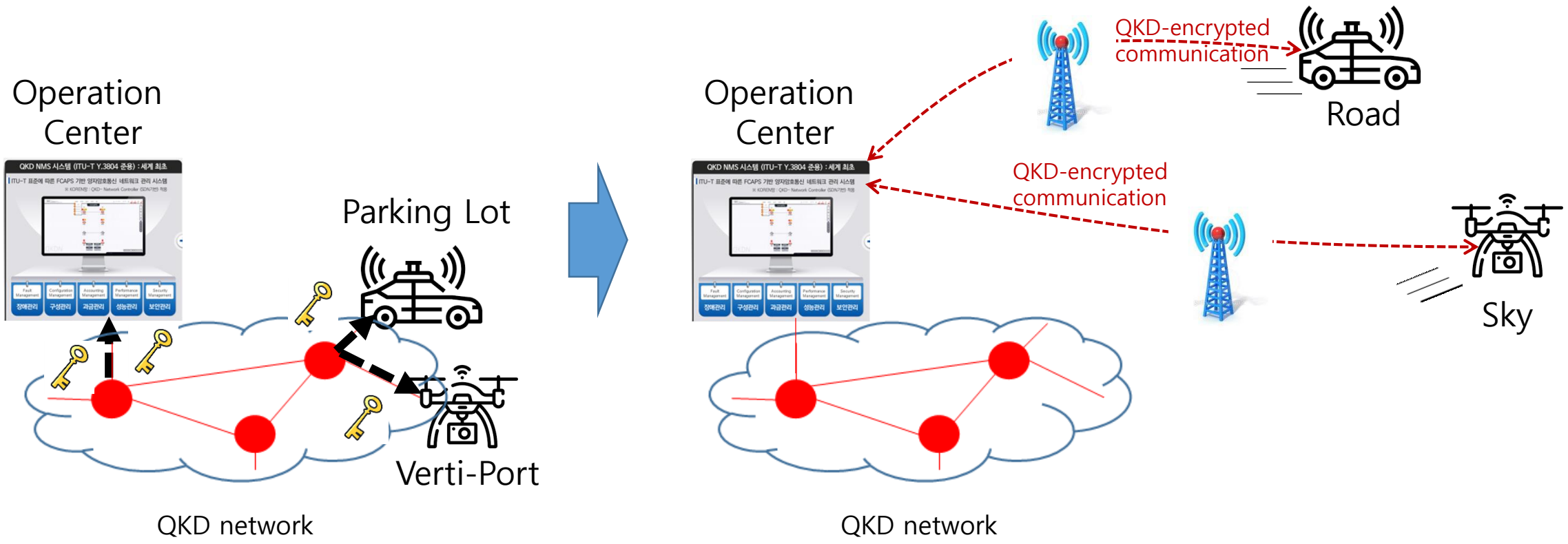


<Quantum- Drone>

2022

Tentative solution in real field

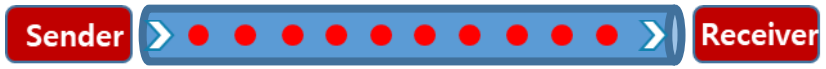
Supplied keys in Fixed, then QKD-encrypted communications in Mobile



Issue on Quantum Channel

Difficulty of receiving single photons in a moving object

Fixed wire



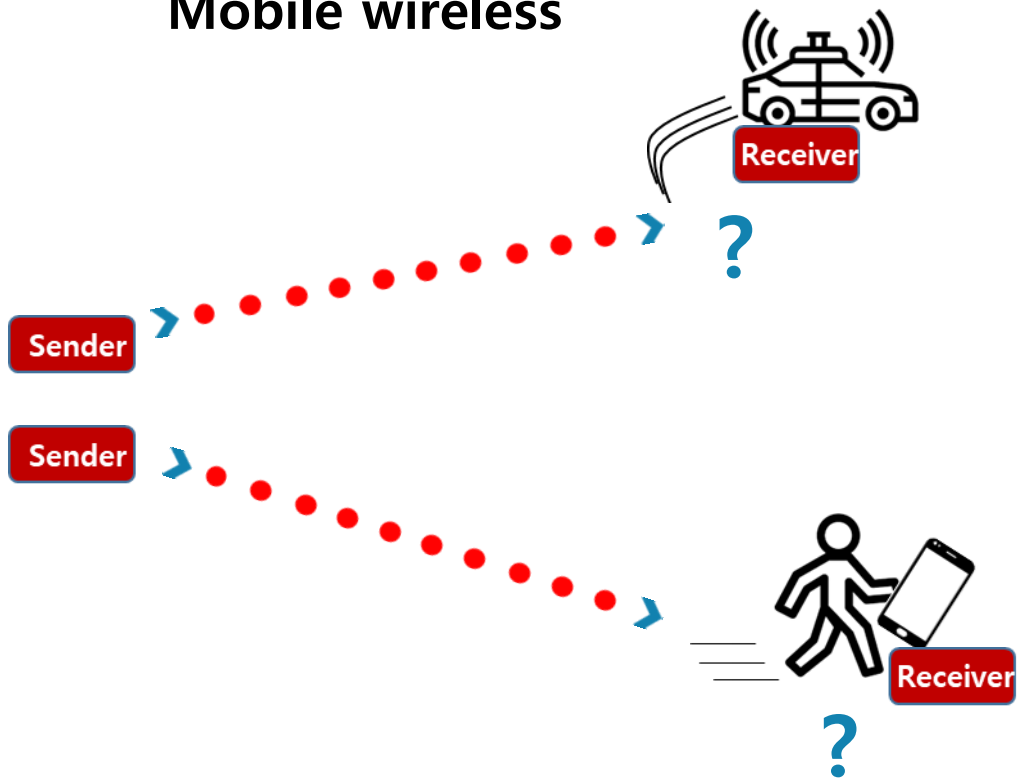
<Optical Cable>

Fixed wireless

<Free Space>

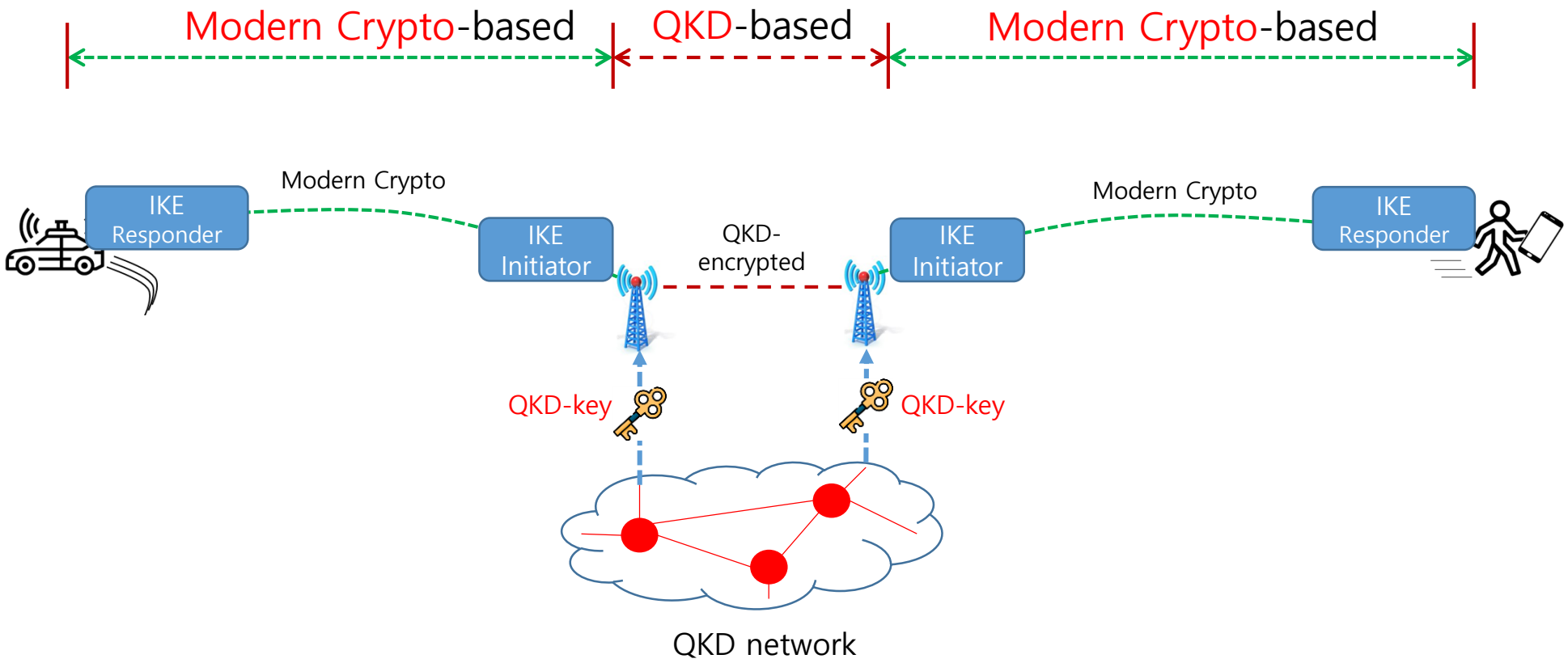
VS.

Mobile wireless



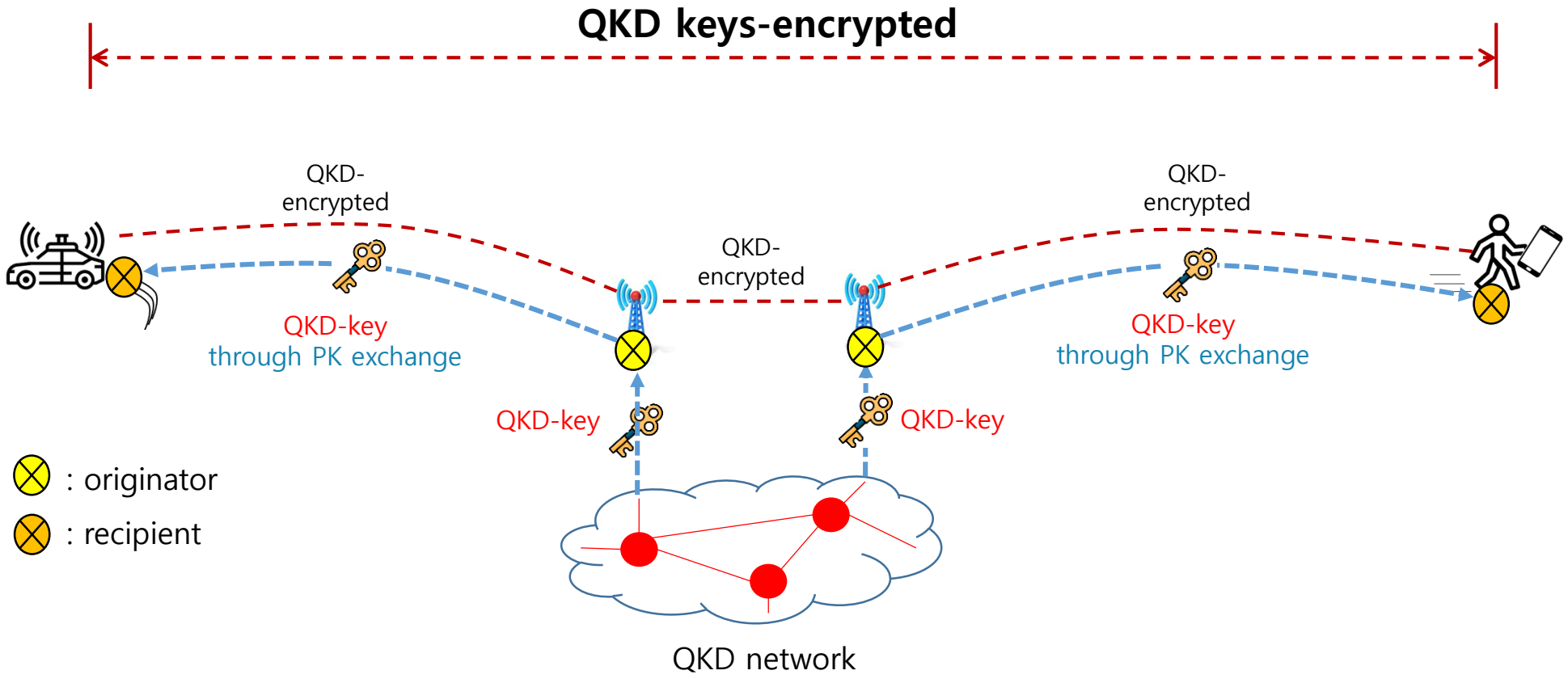
TR of SG13 (Integration of QKD-network with non-QKD tech.)

1. Concatenated scenario with Modern Cryptography



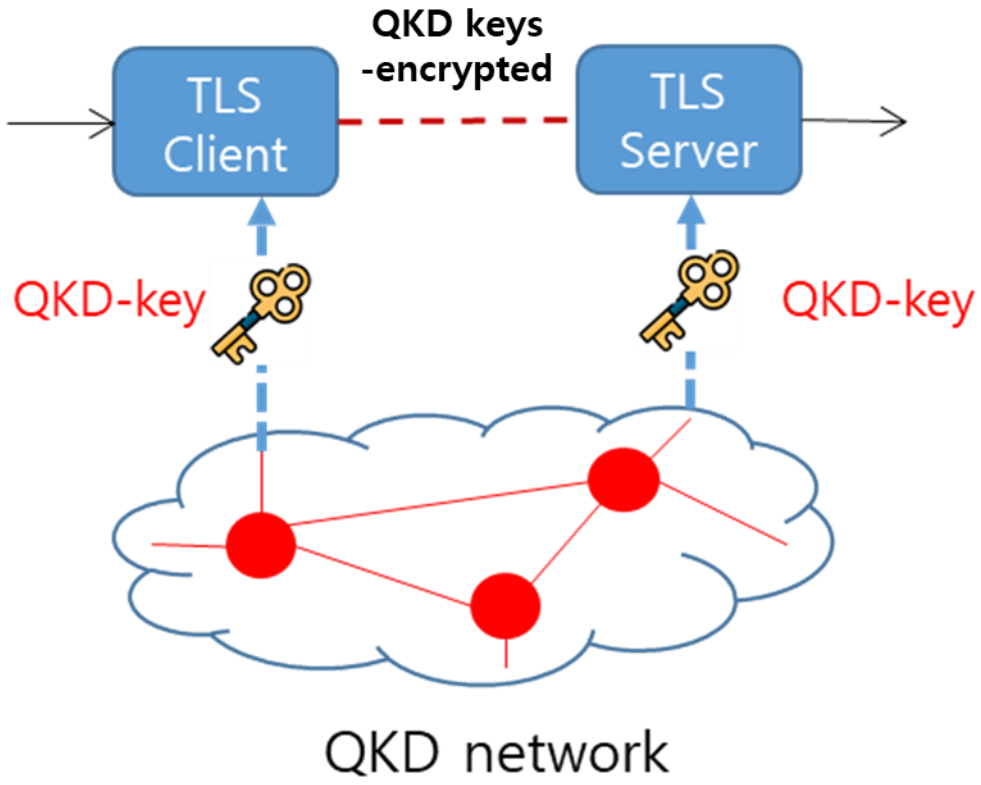
TR of SG13 (Integration of QKD-network with non-QKD tech.)

2. E2E QKD-encrypted scenario through Public Key (key exchange only)



TR of SG13 (Integration of QKD-network with non-QKD tech.)

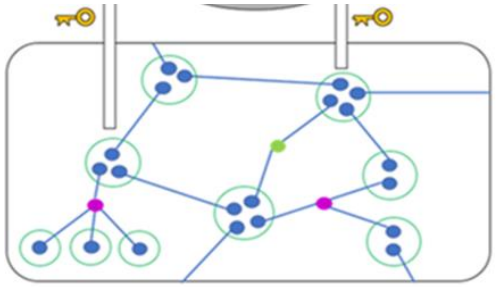
3. QKD keys-used Modern Cryptography



Example of QKD with X.509 (1)

QKD tech. supports only

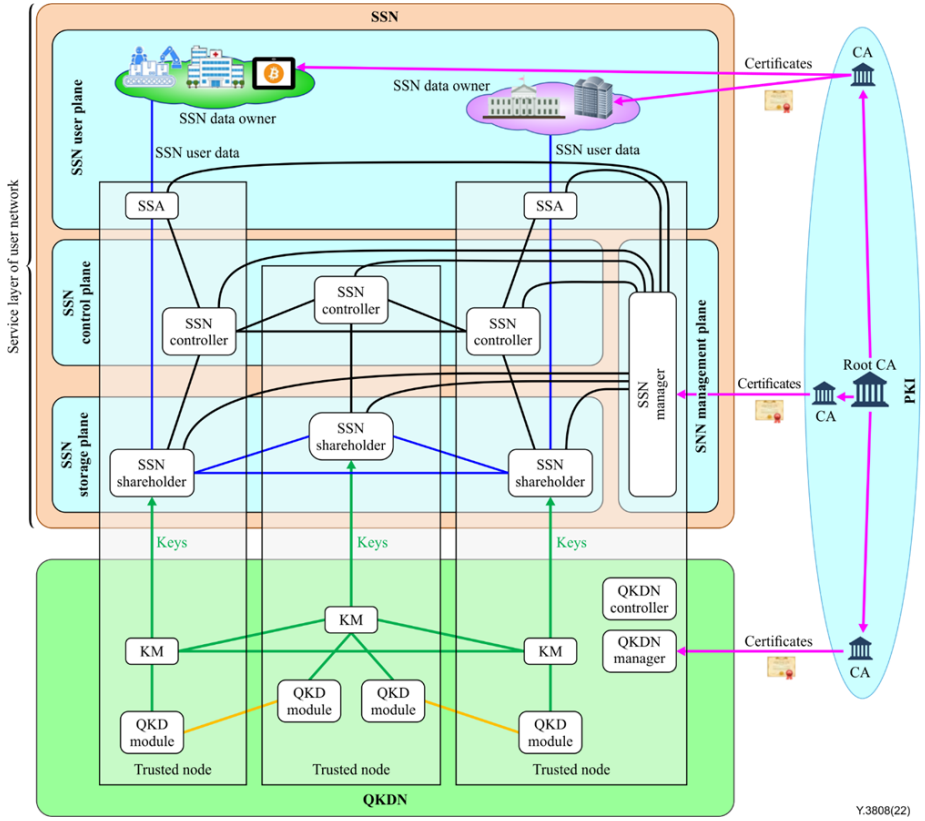
"Key gen. & exchange"



Authentication

for QKD network

- **Rec. Y.3808,** PKI-based QKDN implementation scenario

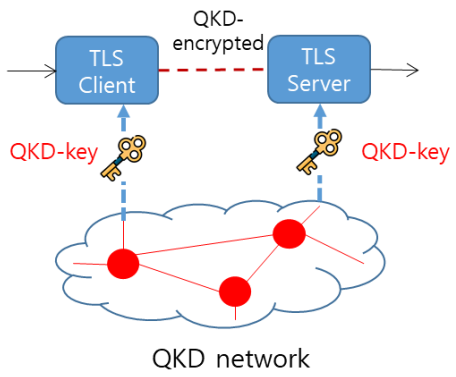


- **Rec. X.sec_QKDN_AA,**
  Authentication & Authorization for QKD network elements

Example of QKD with X.509 (2)

QKD tech. supports both of

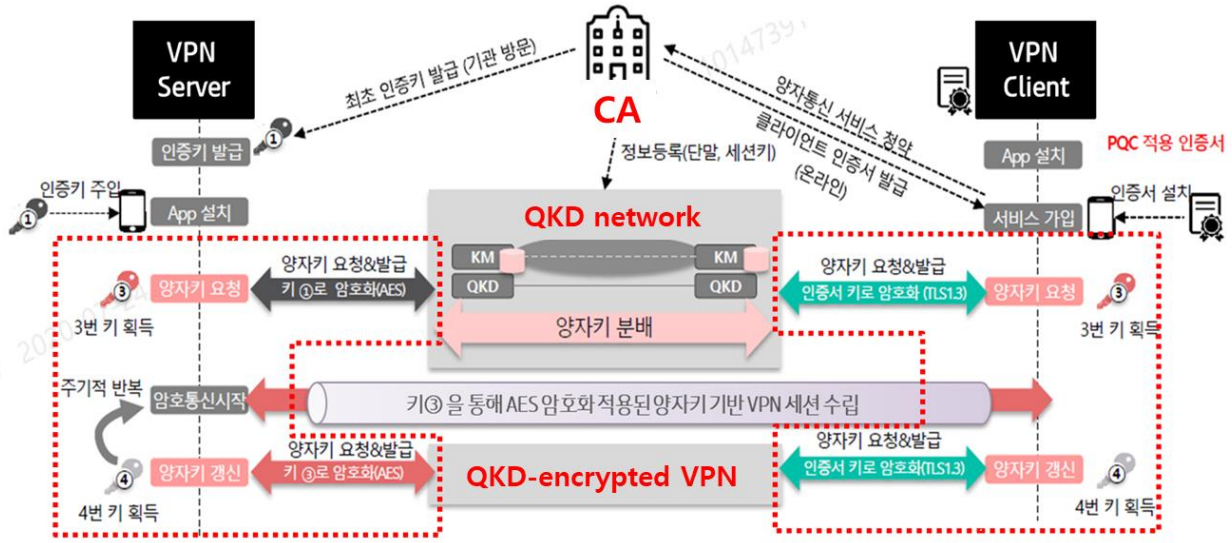
"Key gen. & exchange"



Integration with

Modern Crypto protocols

- **Quantum-VPN,** KT's commercial service launched in 2022



※ 'Key Generation and exchange' procedures are unnecessary in modern crypto protocols

Three implications

1. Integration with X.509 is essential

- for authentication and authorization for the purpose of QKD service

2. X.509 should be taken into account quantum-safety

- collaboration with PQC algorithms* and QKD tech. could be a good example

  * In addition to PQC from NIST, KpqC is developed in Korea

3. Modification* of Modern Crypto Protocols should be considered

- for the integration with QKD tech.

  * new interface receiving QKD keys from QKD network

  * simplification of protocols (getting rid of key generation and exchange functions)

감사합니다

PEOPLE.
TECHNOLOGY.