# 글로벌 ICT 표준 컨퍼런스 2023

Global ICT Standards Conference 2023

(세션1) 양자기술: 디지털 세상의 새로운 패러다임

# 양자암호 보안 표준화 동향

## - QKD/PQC 및 하이브리드 보안 -

심동희, 팀장, SK텔레콤

주최 과학기술정보통신부 Ministry of Science and ICT
특허청 Korean Intellectual Property Office
주관 국립전파연구원 National Radio Research Agency
TTA IITP KEA kista ETRI

# Index

# Index

# 01. Integrating QKD with Encryption Solutions and Operators' Networks to provide End to End Network Encryption

## End to End Network Encryption

### Integration with Operators' Network

**Centralized Control**

- Interoperability between different QKD Systems
- Control and Management based on International Standards to make sure the global reach and interoperability

### Integration with Encryption Solutions

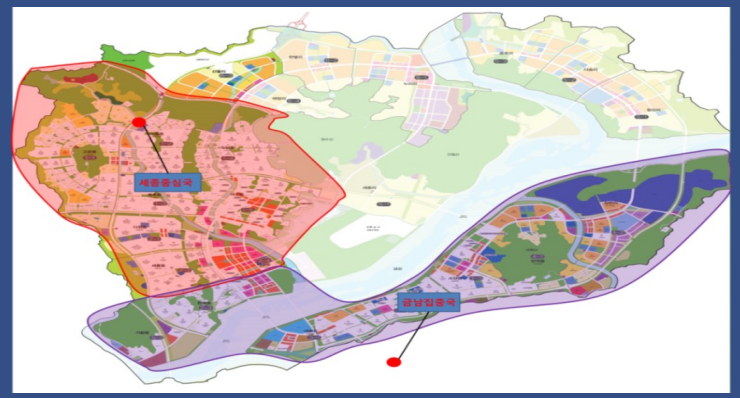
**End to End Encryption**

- Network Encryption Upgrade with QKD
- Work with PQC - Hybrid solutions with QKD and PQC

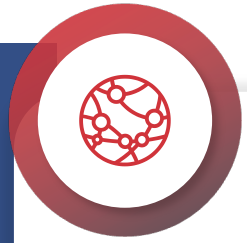
# 02. SKT' World first LTE Backhaul Protection with QKD

World-First (June '16)

## LTE backhaul Protection with QKD



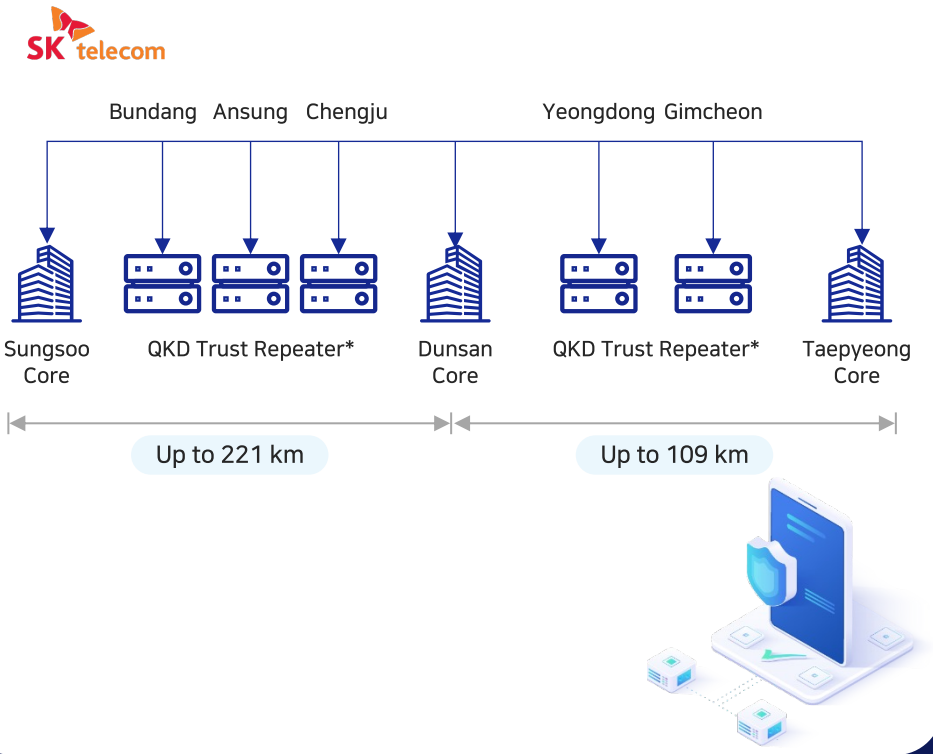
Configuration of
QKD Network in Sejong



# 03. SKT's 5G Backbone protection with QKD

5G Backbone protection with QKD since 2019


## Quantum-safe Network with QKD



# 04. Korean Convergence Network for e-Government

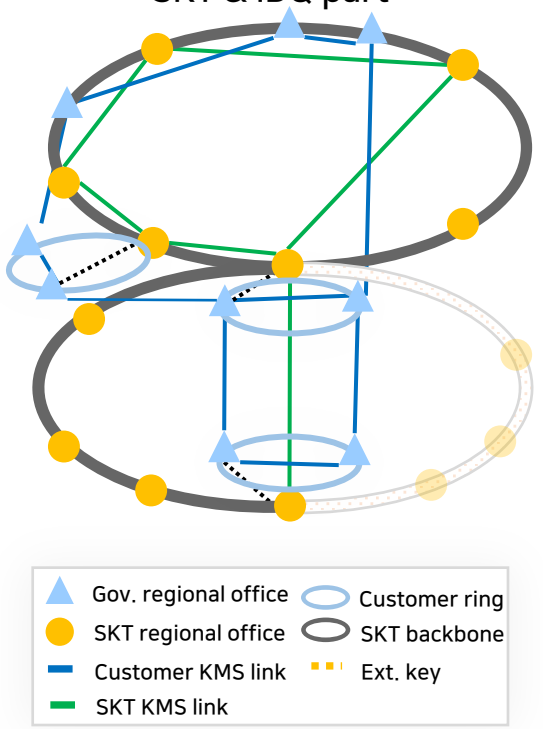
## Government Convergence Network with highest level of Security

Construction of the first nation-wide Government QKD network in Korea

A national backbone network interconnect individual networks run by 48 government organizations

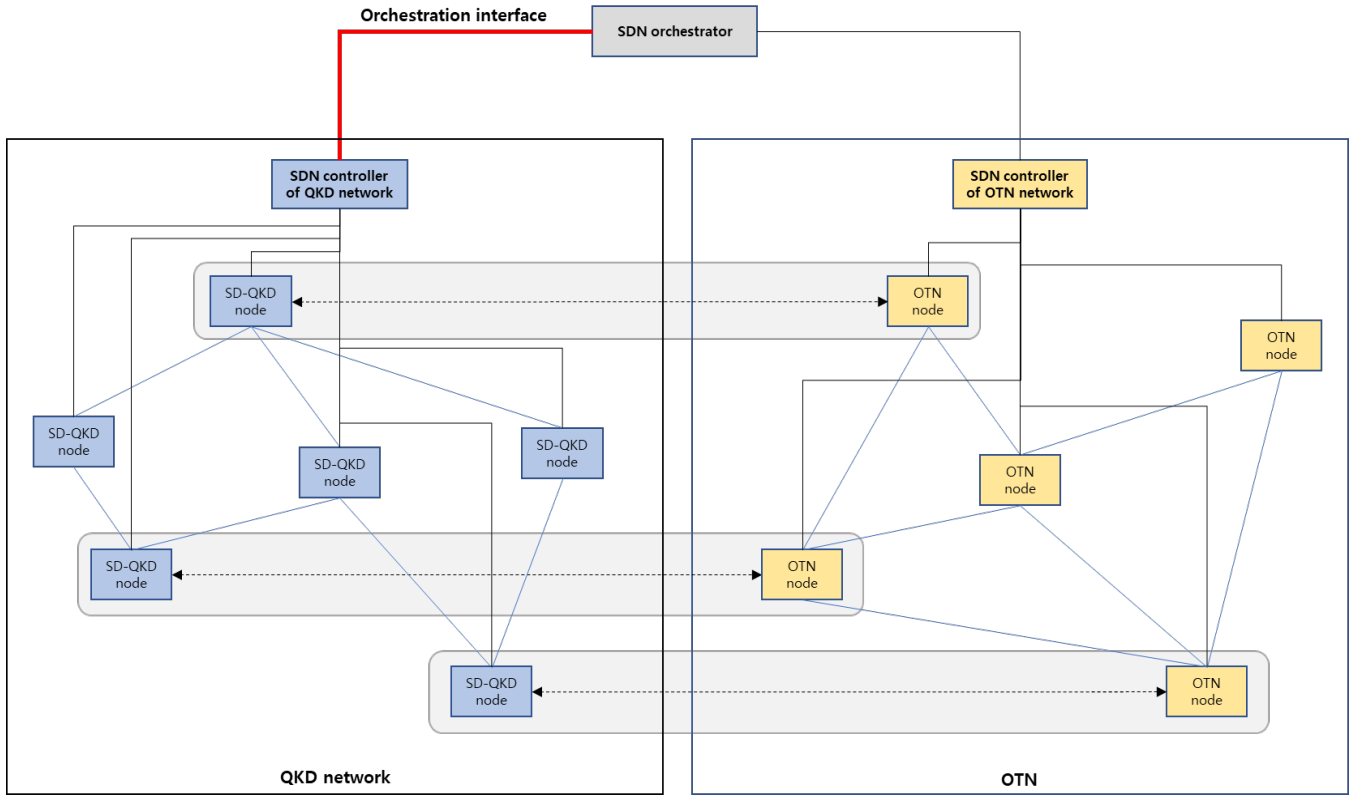
- 800 kilometers
- 48 government organizations
- Security, stability & efficiency

[ QKD & KMS Network ]
SKT & IDQ part



# 05. Orchestration Interface for Software Defined Networks

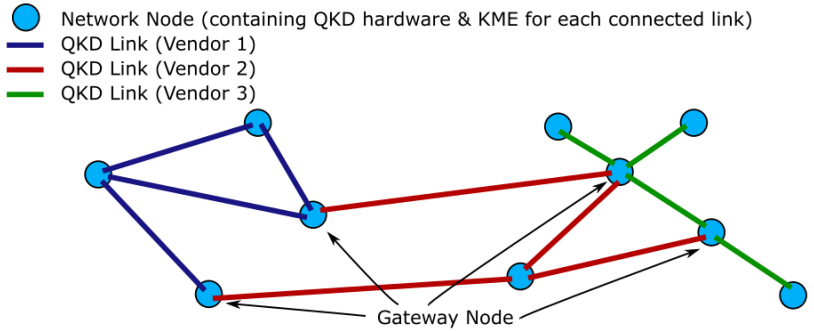
## ETSI GS QKD 018

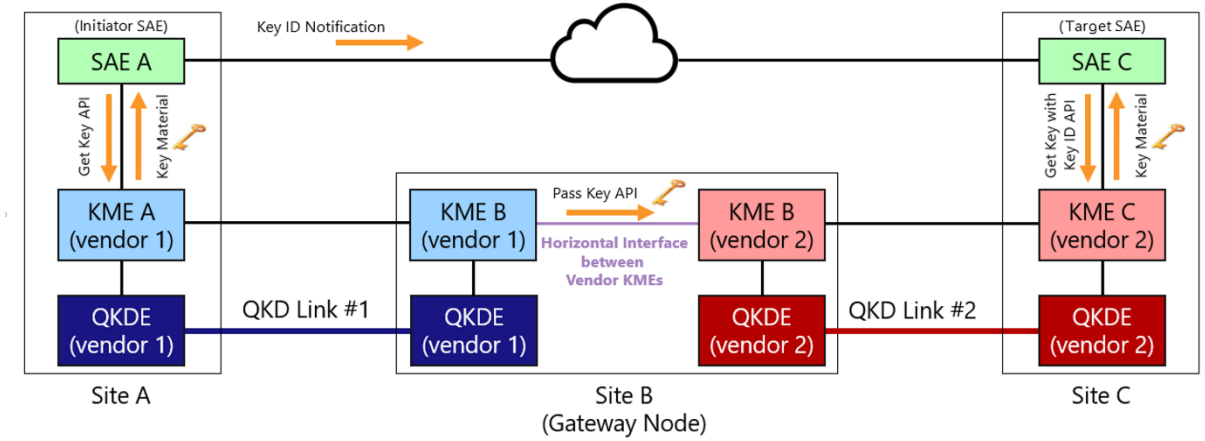



- SDN Orchestration for QKD
- SDN Orchestration Interface, Service provisioning
- Sequence diagrams
- YANG Model

# 06. Protocol and data format of REST-based Interoperable Key Management System API

## ETSI GS QKD 020

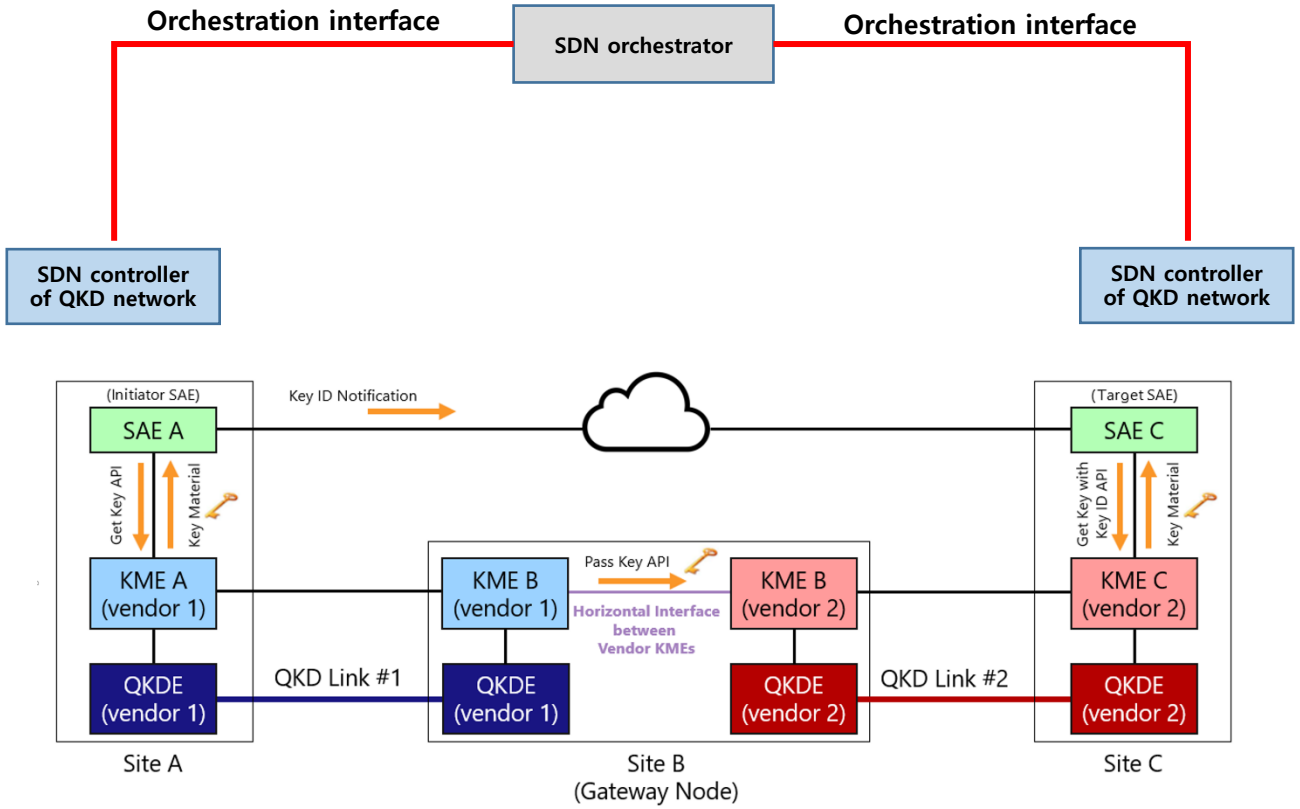



- REST API allows key management systems to interoperate to pass keys horizontally between two systems located in a common trusted node

# 07. Orchestration Interface for the Interoperable KMS

## ETSI GS QKD 021




- Interface between the SDN Orchestrator and the SDN Controller of QKD networks for interoperable key management between two QKD networks
- YANG model etc

# Index

# 08. Migration

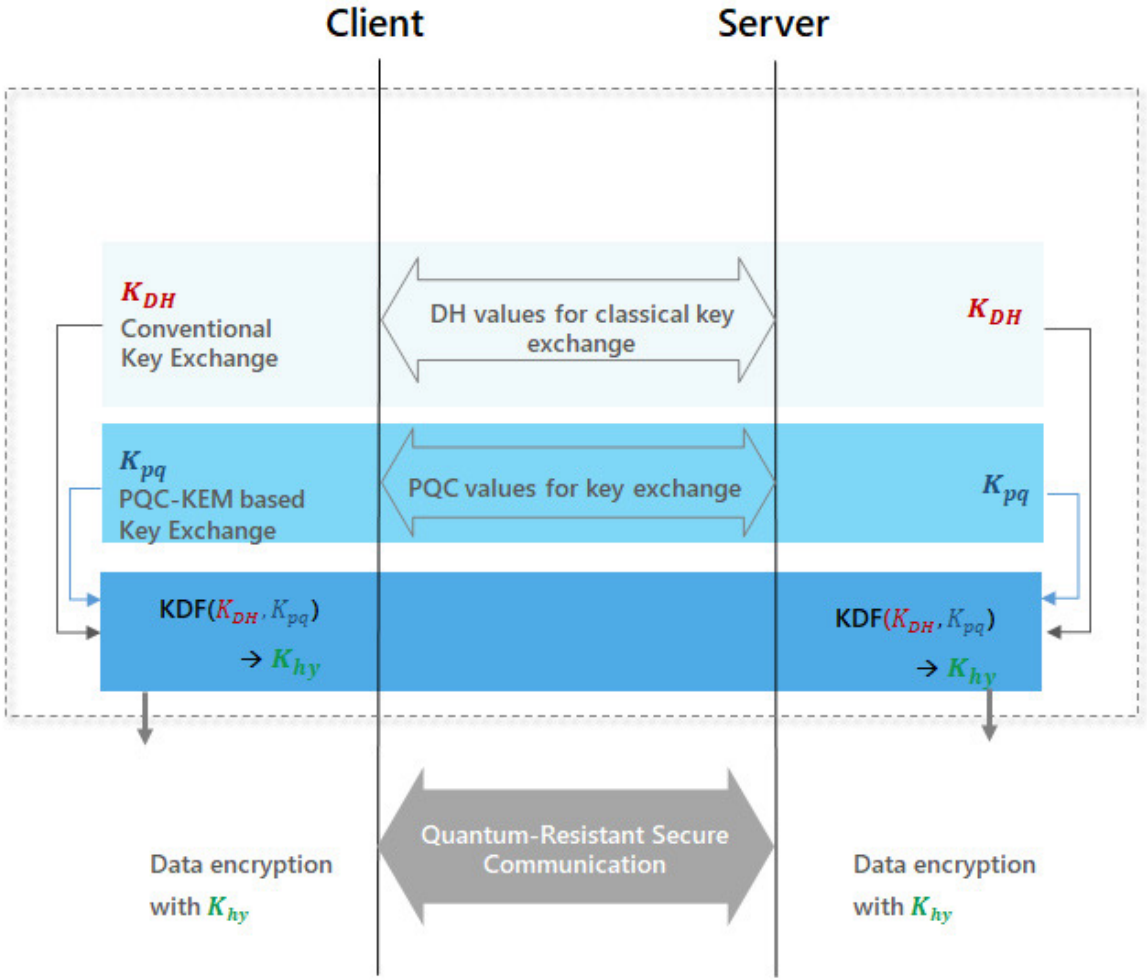
| | |
|---|---|
| AES Migration | DES / 3DES → AES(2001) (on-going) +20 years |
| SHA2/3 Migration | SHA-1 → SHA2/3 (2011) +20 years |
| ECC Migration | Not mandatory, fairly easy |

# 09. Migration to PQC

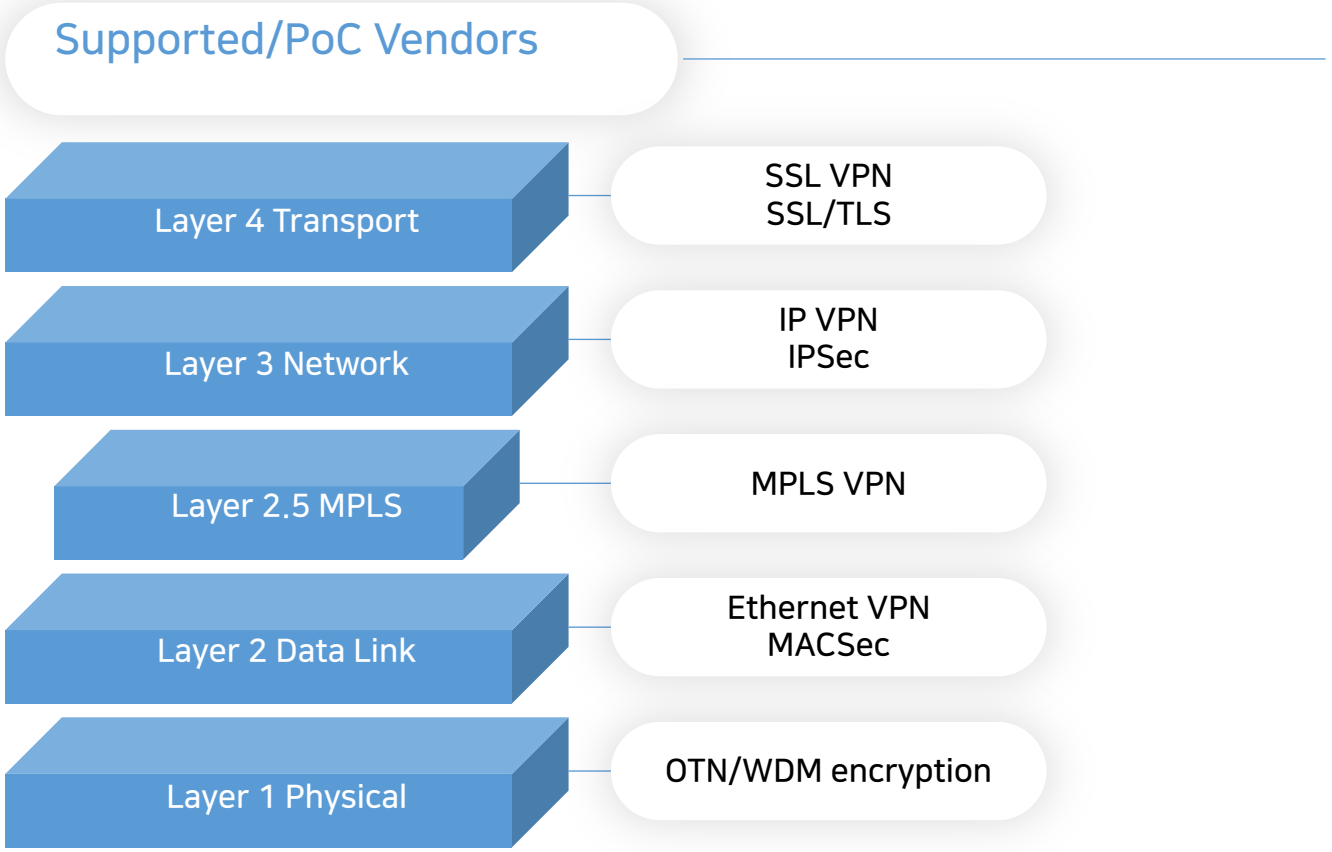
## 3 Pillars

| Algorithm | Protocols | System |
| --- | --- | --- |
| PQC Standardiza-tion (NIST) | PQC-enabled protocols | PQC support to PKI/CA, HSM, process |

# 10. PQC – Classical Hybrid



# 11. Integrating QKD with existing Encryption Solutions

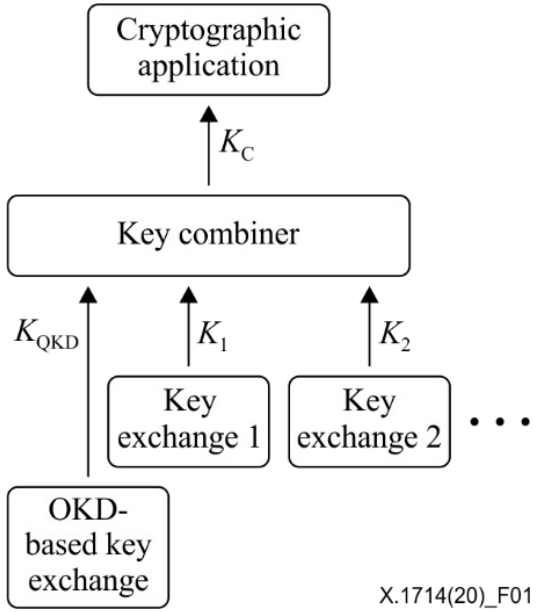


# 12. ITU-T SG17 Overview of Hybrid approaches for key exchange with QKD

| | |
|---|---|
| ITU-T SG17 | X.1714 |
| ETSI | TS 103 744 (concatenate / cascade hybrid key exchange) |
| IETF | RFC 8784 (mixing pre-shared keys for PQC) |

# 13. ITU-T SG17 Key Combination and Confidential Key supply for QKD Network

## Key combination method

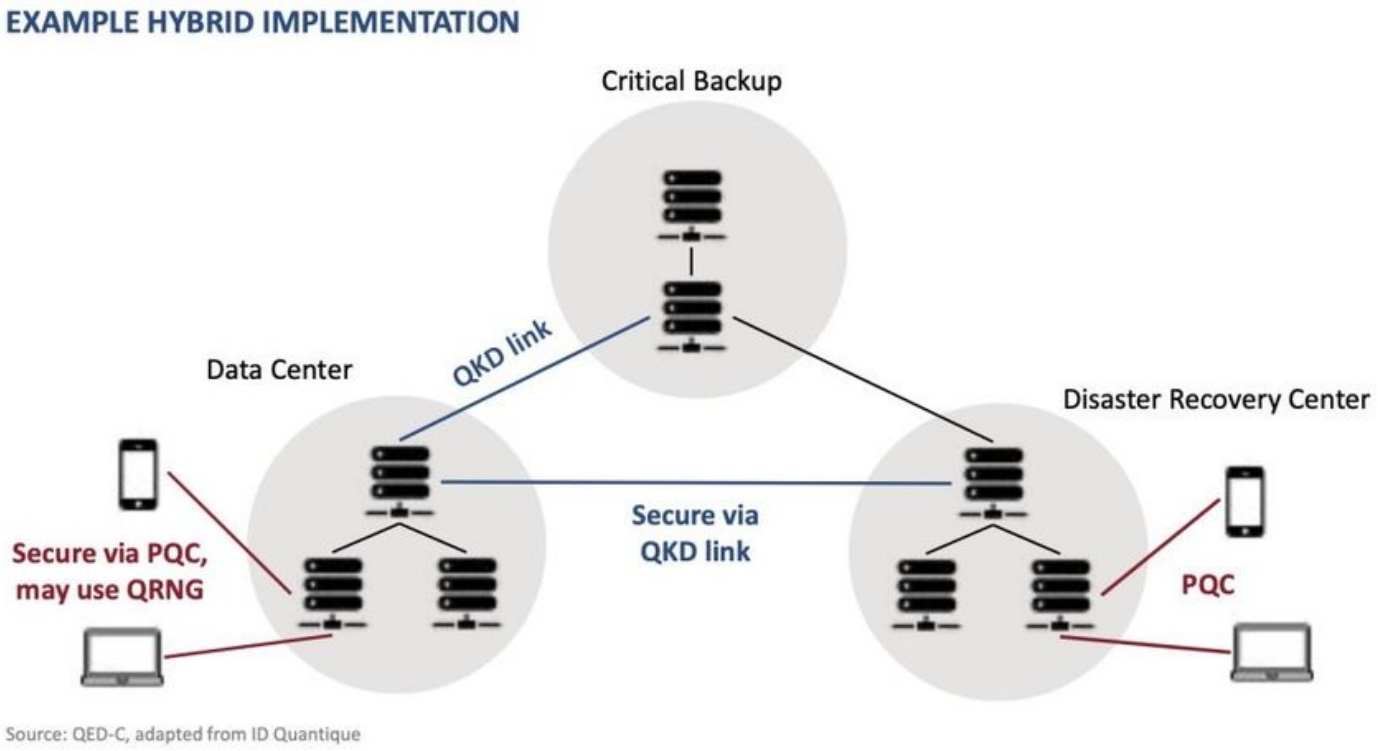



## Security requirements for key combination

## Security requirements for key supply

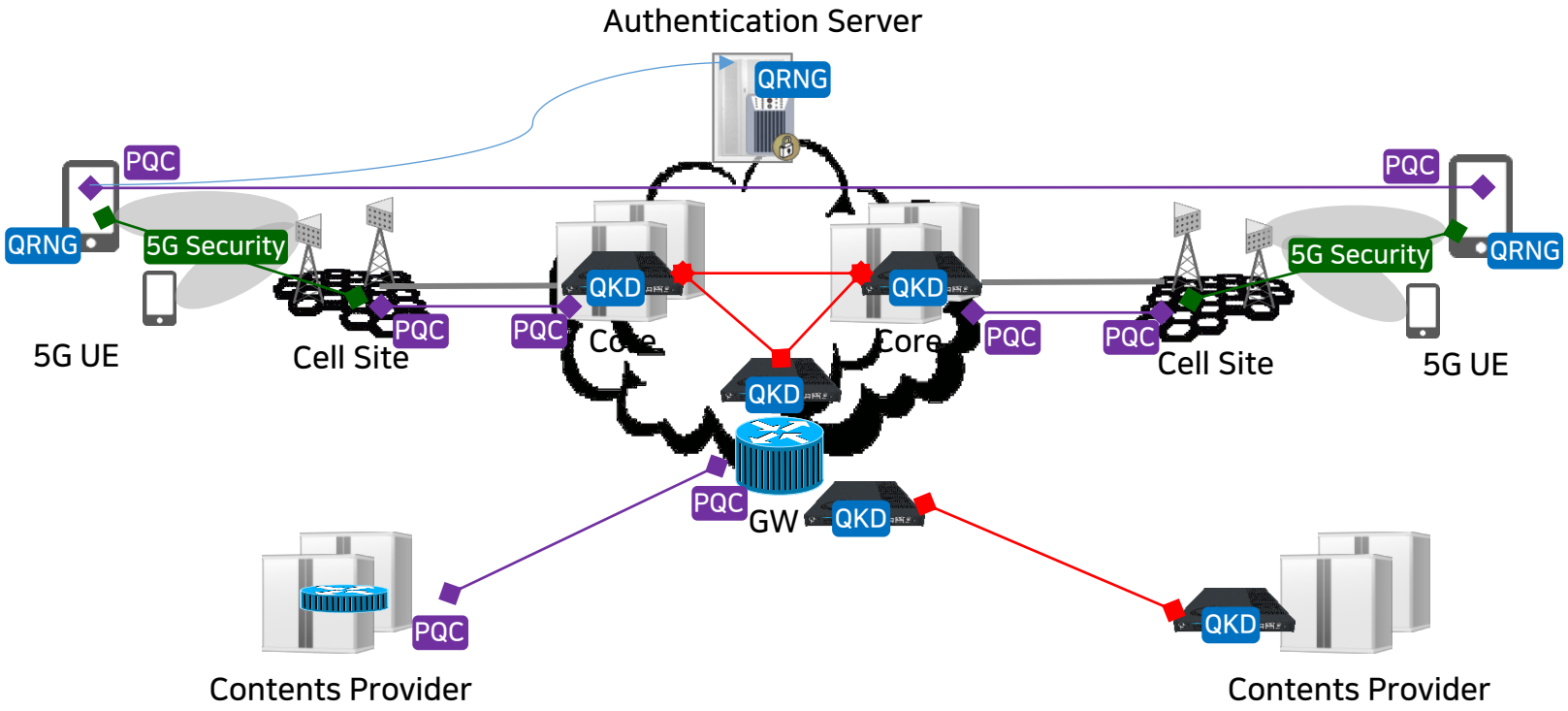
# Index

# 14. ITU-T SG17 Overview of key management of hybrid approaches for quantum-safe communications




Example

# 15. QKD-PQC Hybrid Implementation Example




# 감사합니다.

심동희, 팀장, SK텔레콤
donghee.shim@sk.com