Introduction of PQC pilot infrastructure and services in the industrial area

LGUplus

*Kyoung Hak Mun

CONTENTS

CHAPTER

I Introduction

Quantum Computer and Security Threats

"If large-scale quantum computers are ever built, they will be able to **break many of the public-key cryptosystems** currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere."

-Post-Quantum Cryptography, Overview, NIST-

IBM Q System One

Google

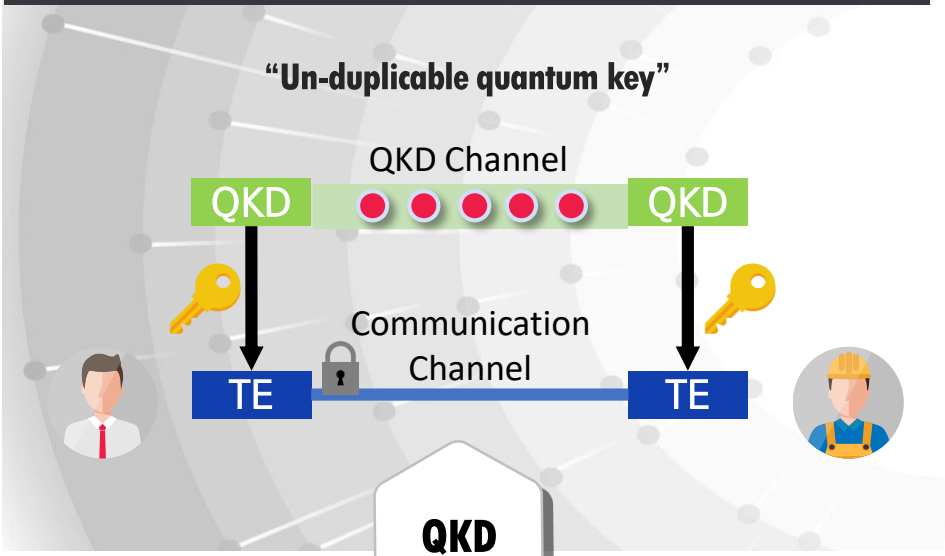
"Google has begun building a new and larger quantum computing research center that will employ hundreds of people to design and build a broadly useful quantum computer by 2029." – I/O 2021 summit, google-

"IBM is installing its first commercial quantum computer at the Cleveland Clinic this year(2021)"

Quantum Security

Quantum-physical QKD

Quantum key

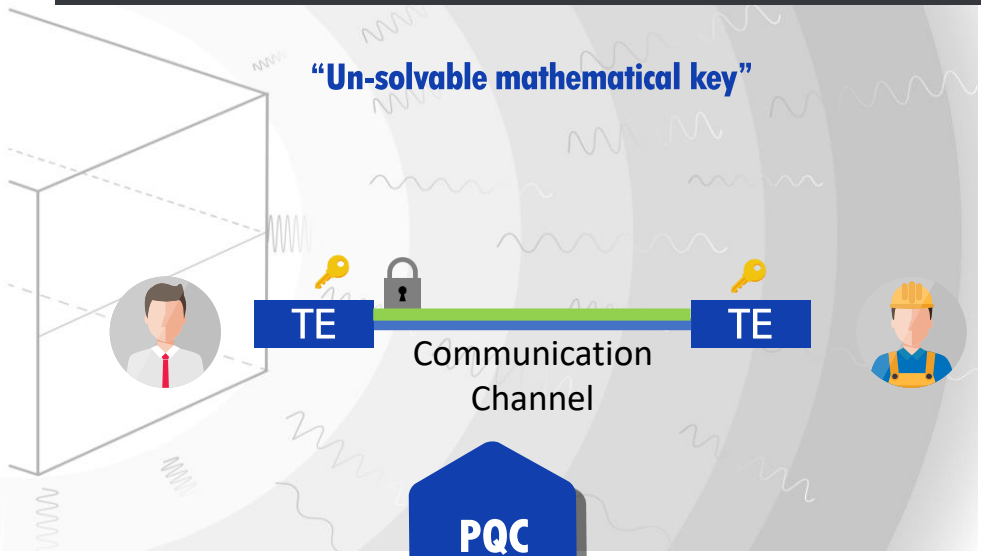


QKD

- Key exchange using the quantum of single photons
- QKD equipment and dedicated line required
- Limitation of delivery media (optical fiber, air)
- Limitation of transmission length
- Key exchange only

Mathematical PQC

Digital key



PQC

- Key exchange using un-solvable problems by quantum computer
- Variable applicability in the form of software
- Key delivery through various media
- Upgrading modern cryptosystem to quantum security

Quantum Security Roadmap of LGUplus

U+ PQC Roadmap

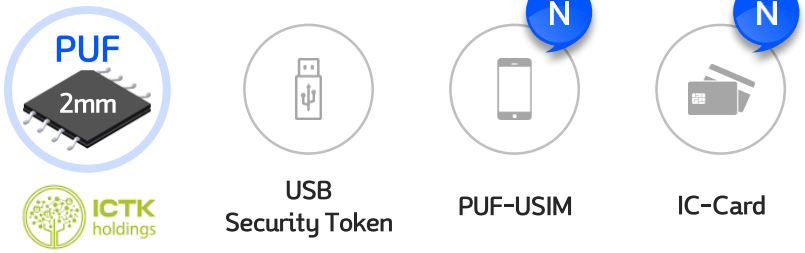
’18년	’19년	’20년	’21년
PQC Transmission Equipment	PQC TTA Standard	PQC Service References	PQC Extended Applications

* TTA: Telecommunications Technology Association

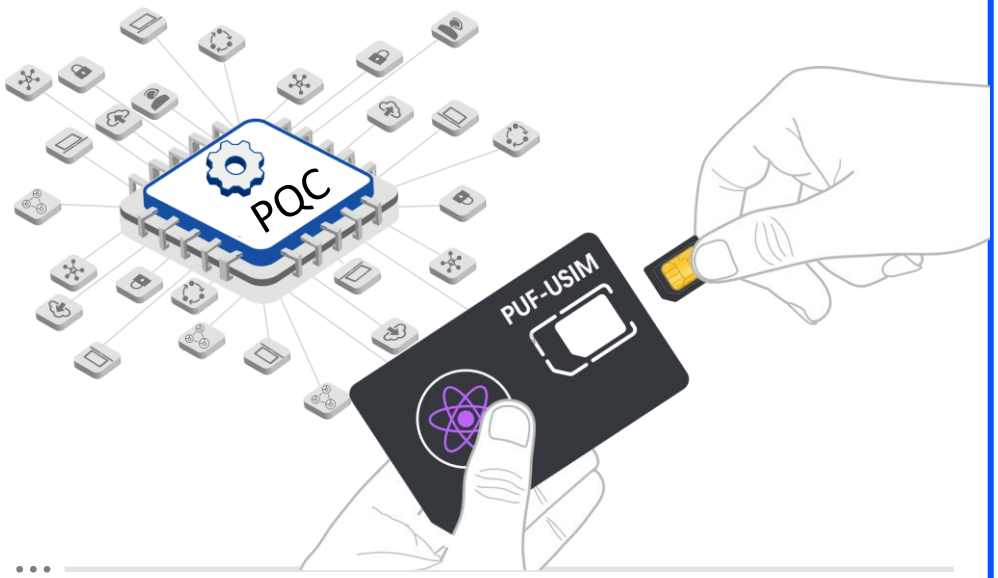
- Development of PQC-based optical transmission equipment
- PQC-based private network service
- Development of PQC-based industrial application

PUF Roadmap

* Physically Unclonable Function



- Secure protection of certificate private key
- Applicable to smartphone and IoT devices authentication



Quantum Security + Enhanced Authentication

Cloud Computing | Un-tact Performance | Un-tact Medical care | Un-tact Financial services

CHAPTER

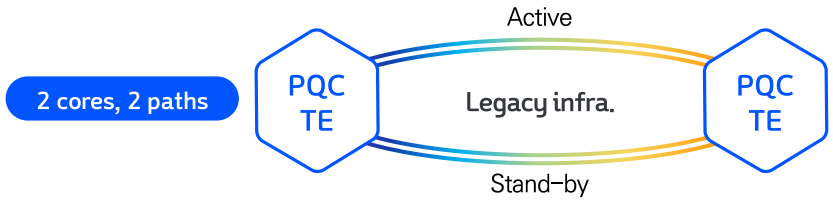
II

Advantages of PQC

PQC applicable to various network topology

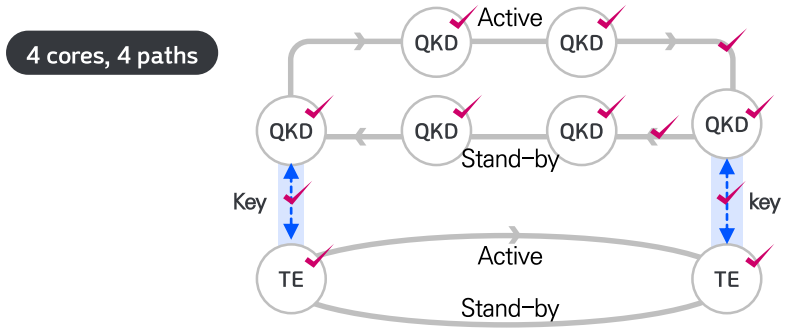
Capable to configuration by existing network infrastructure

Transmission network configuration for PQC



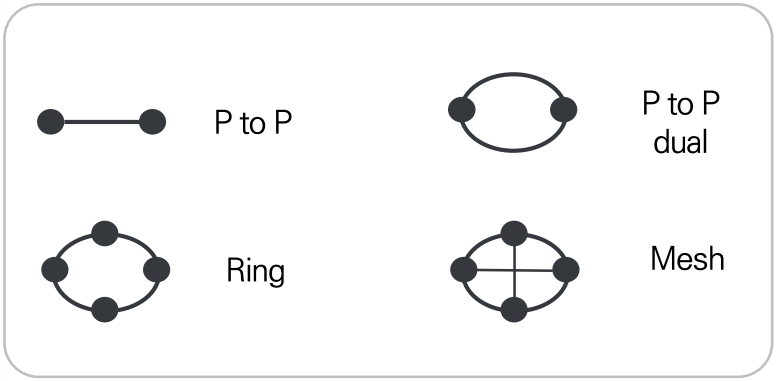
- Communication network and key distribution network using one infrastructure

Note: QKD



- Requires separate key distribution infrastructure

Variable network topology

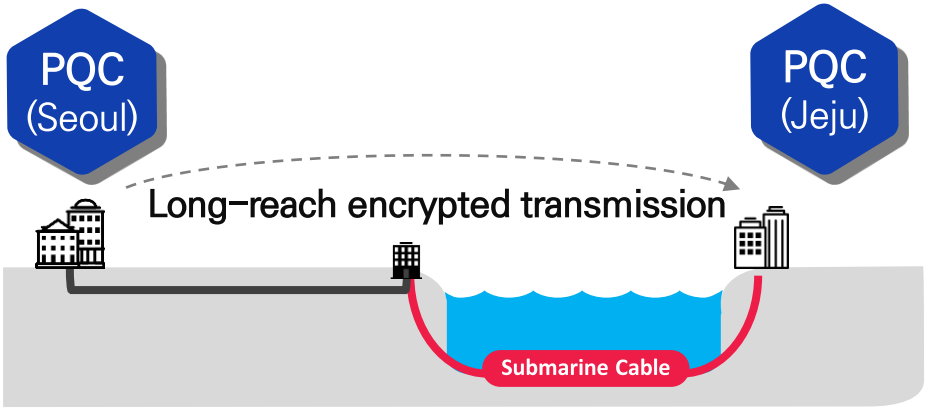


Capability to respond to various network environment

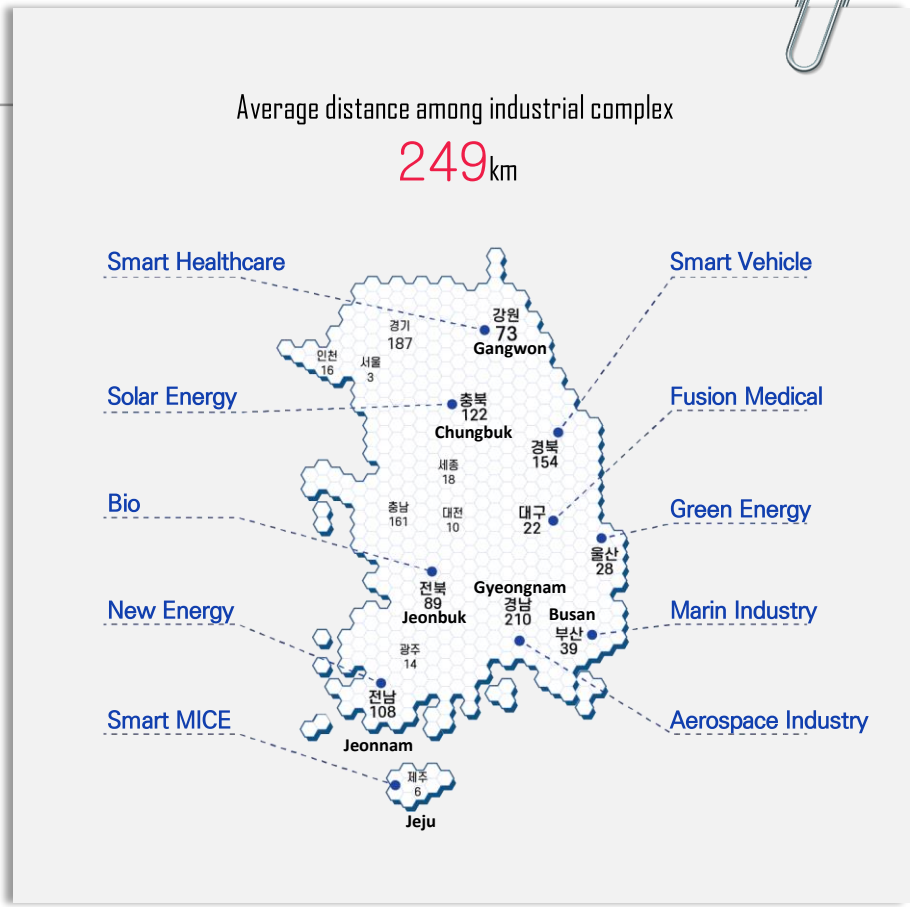
❖ Spreading to various industry

PQC capable of encrypted transmission over long distances

Encrypted private network service without distance limitation



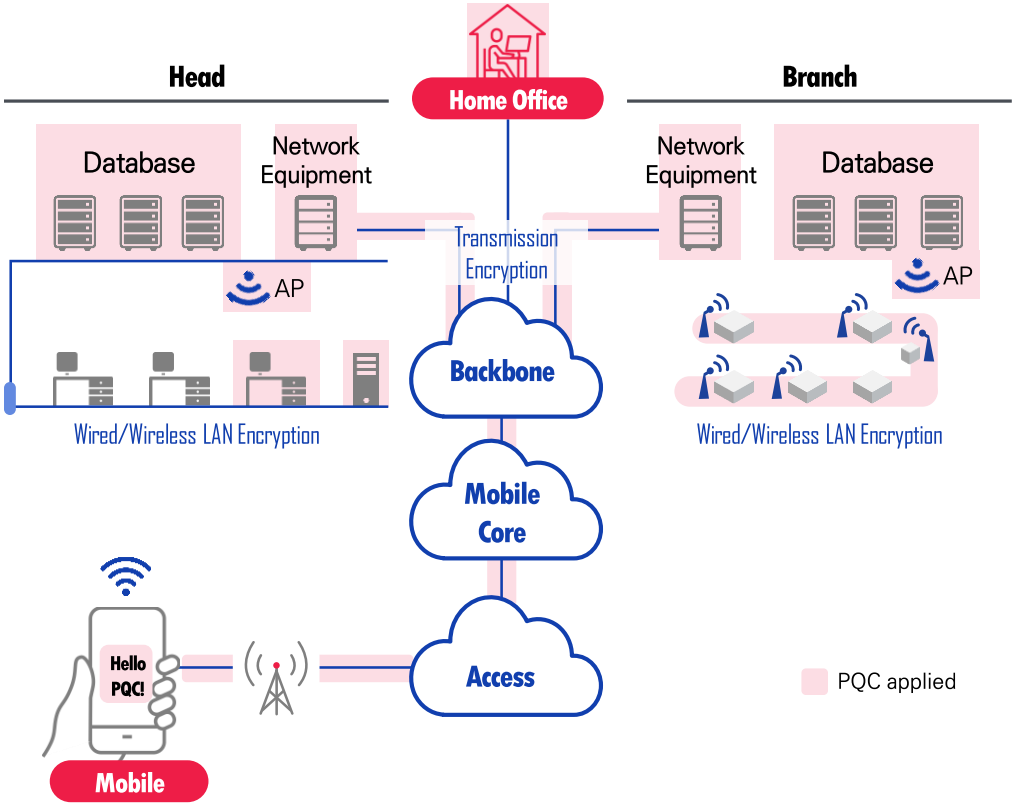
- More than 500km of transmission distance required for connection between most industries in Korea
- Requires a stable key exchange network that allows the use of submarine cables



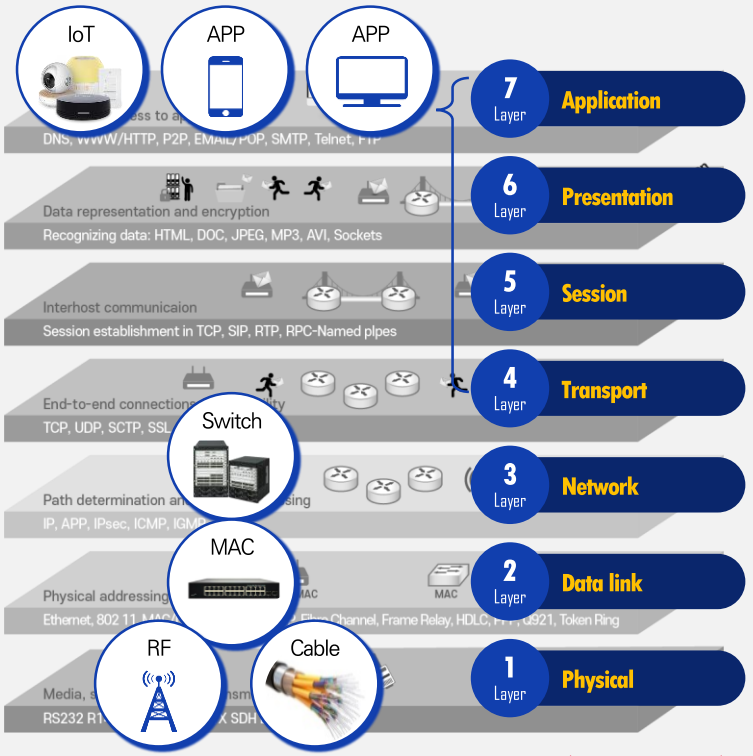
PQC applicable to various network services

PQC algorithm can be applied to various network layers

PQC application example in home office and wireless environment



Applicable at all network levels



(OSI 7 Layer)

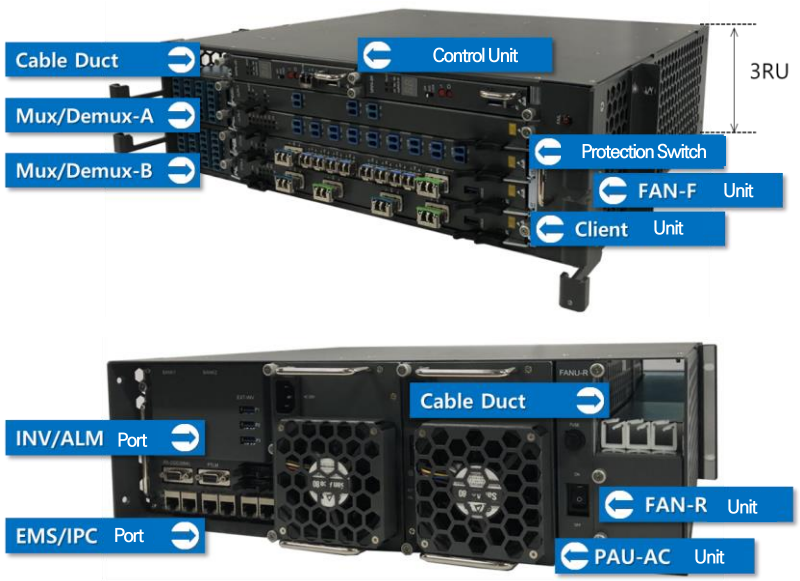
CHAPTER

III PQC pilot services

PQC applied optical transmission equipment

Quantum security transmission service is provided as a single equipment with an embedded PQC module

✓ Transmission Equipment(UTRANS-6300p, *ROADM)



✓ PQC transponder (10Gx4port)

- Provides 4 port of 10G encryption
- Provides Layer1 quantum security
- QRNG for secure key generation
- R.Lizard applied, TTA standard PQC algorithm

  * TTA (Telecommunication Technology Association, Korea)
- Physically protected Crypto. Module
- Low encryption latency

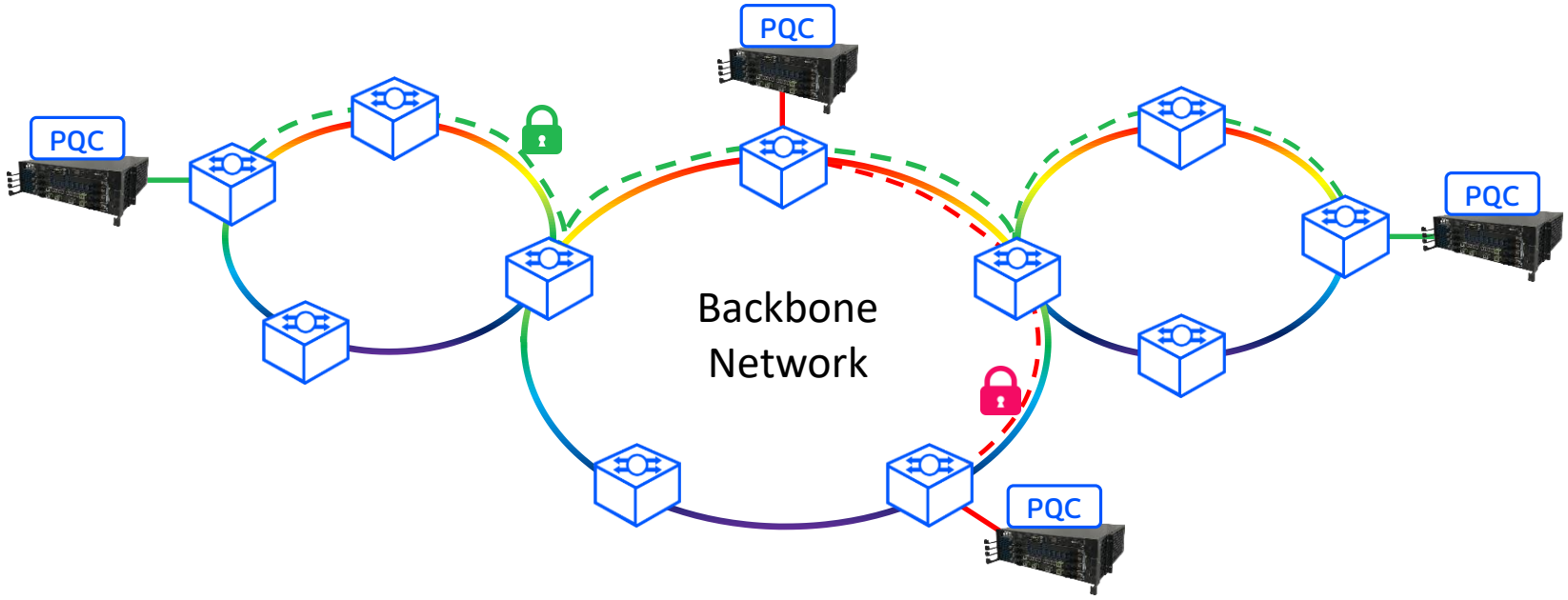
Specifications

- Protection switching
- 9-Degrees, 88 channels (WDM)
- Colorless, Directionless, Flexible Grid
- Fiber channel monitoring

* ROADM (Reconfigurable Optical Add-drop Multiplexer)

PQC transmission network structure

Quantum security is provided by configuring both end-points without additional transmission line and relay node in the existing transmission network.



- No distance restrictions by encryption
- No topology configuration constraints
- End-to-End key exchange without key relay
- Provides protection switching of encrypted signal
- Applicable to submarine communication cables

Cases of the PQC transmission service implementation

Korean Digital New-Deal, quantum security pilot infra. deployment

1. Use of transmission equipment with embedded PQC
2. Provides protection configuration to ensure service survivability
3. Communication and encryption service integrated control server construction
4. Completion of domestic TTA test

LGUplus
Control & Monitor

PQC Industry

LG Innotek
Camera Module Manufacture

Pyeong Taek
Database
Security Documents

10Gbps
Encrypted by PQC
active
standby

Busan
Database

Section	Distance	Interface	Protection Line
Busan~ Pyeongtaek	636 km	10 Gbps	785 km

Private network
+
PQC security

PQC Medical

EMC 을지병원
EULJI MEDICAL CENTER

Seoul
Database
Patient information

10Gbps
Encrypted by PQC
active
standby

Daejeon

Section	Distance	Interface	Protection Line
Seoul~ Daejeon	207km	10 Gbps	226 km

LG U+

NIA NATIONAL INFORMATION SOCIETY AGENCY

Cases of the PQC application

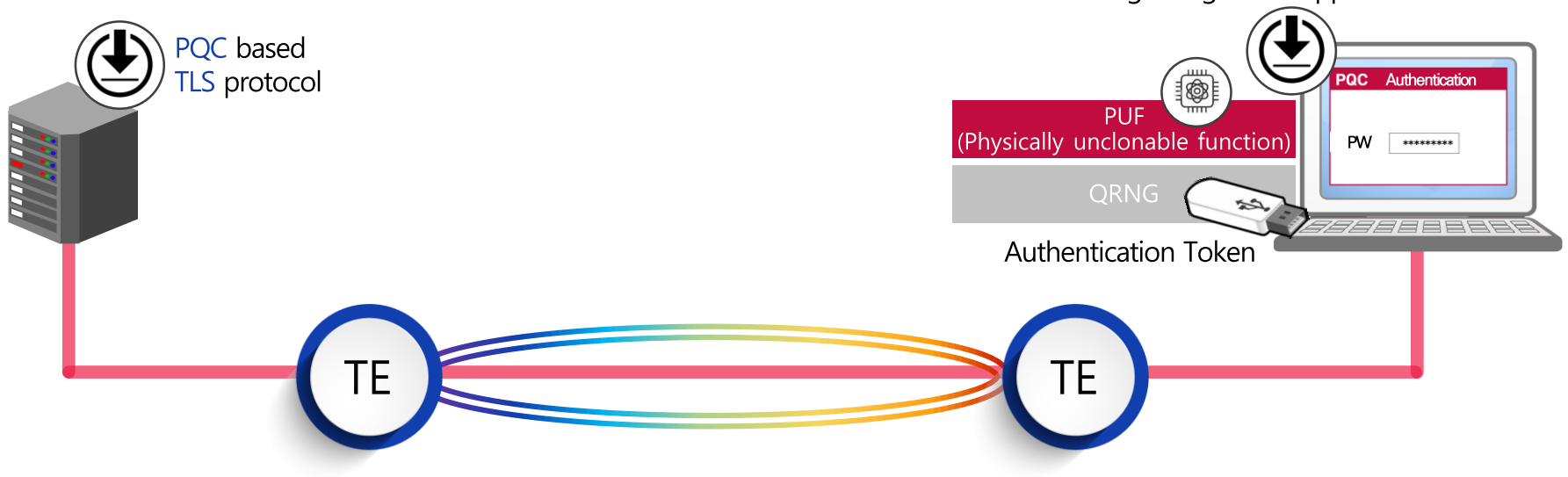
PQC application service for sending and receiving industrial confidential data

1. PQC-TLS applicable to various services

- TLS (Transport Layer Security) with PQC key exchange
  : Can be used for https, SSL-VPN, etc.

2. Service Permissions by Authentication Token

- Small security token with built-in QPUF
  : Prevention of certificate private key theft
  : Modular NTRU based Digital signature applied

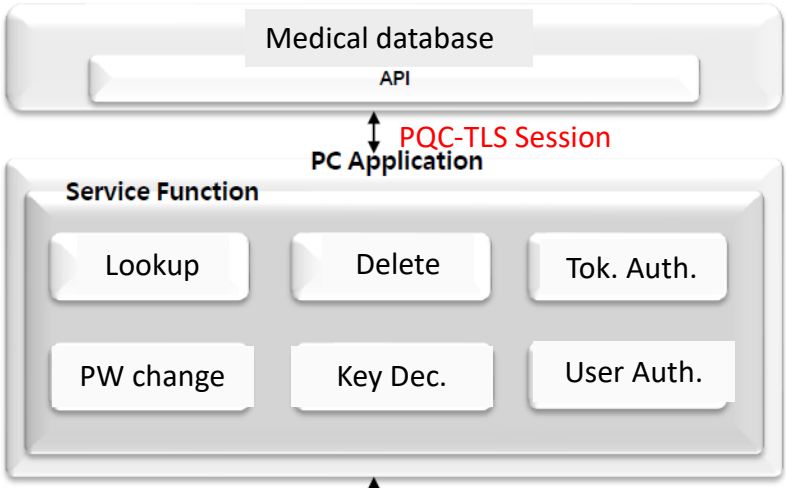


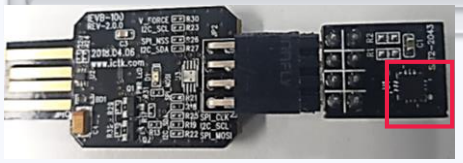
Remote viewing service for patient examination and diagnostic data for EULJI Medical Center

Industry confidential information delivery application for LG Innotek

PQC application for medical center

Medical application configuration





QPUF

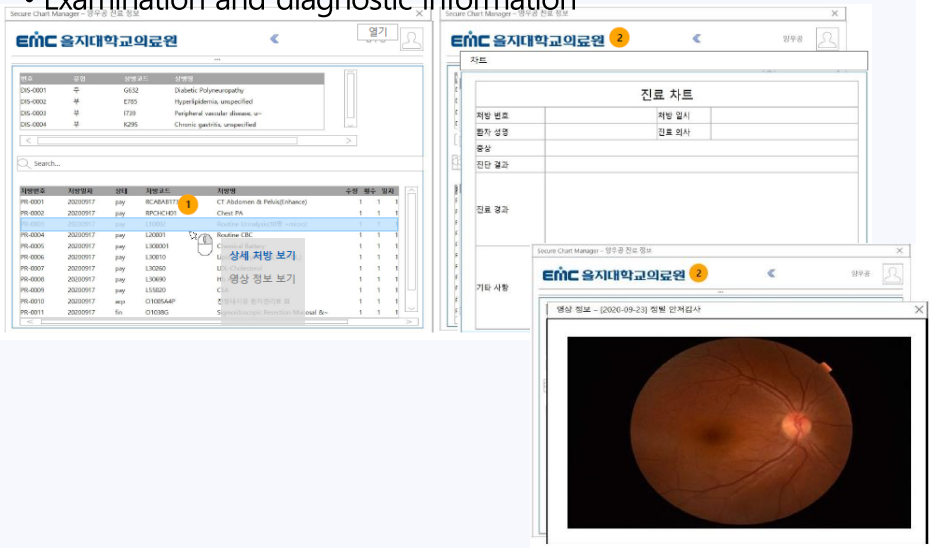
- ✓ QPUF Authentication token embedded
- ✓ PQC certification

Application UI

- QPUF User Auth. Log-in

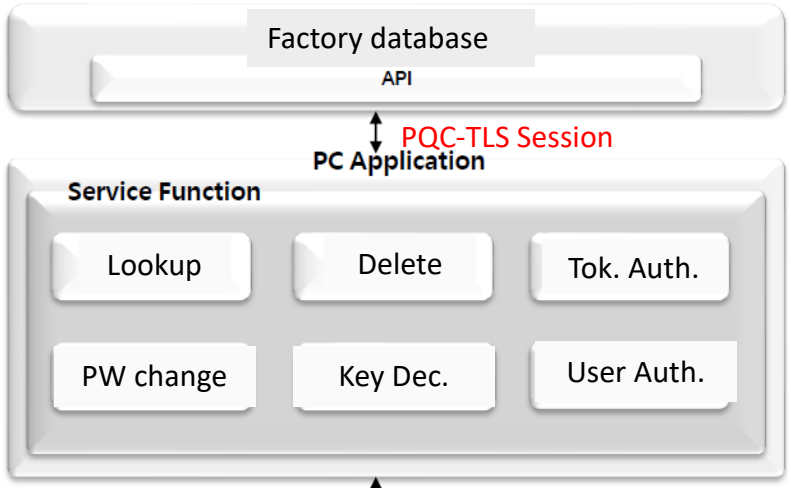
- Patient DB

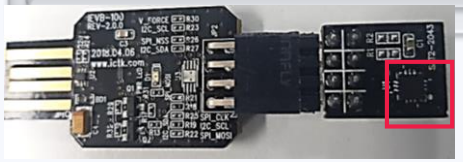
- Examination and diagnostic information



PQC application for factory

Industrial application configuration





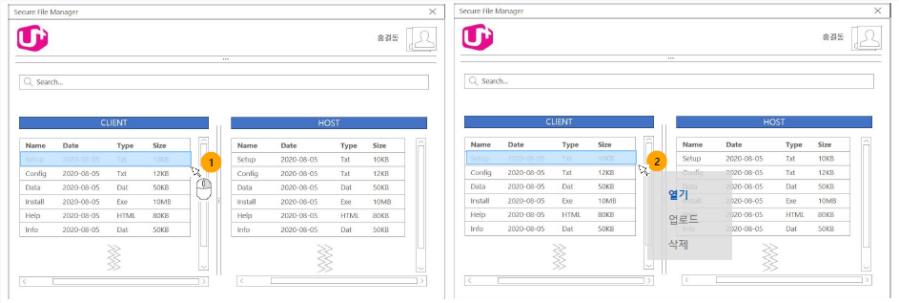
QPUF

- ✓ QPUF Authentication token embedded
- ✓ PQC certification

Application UI

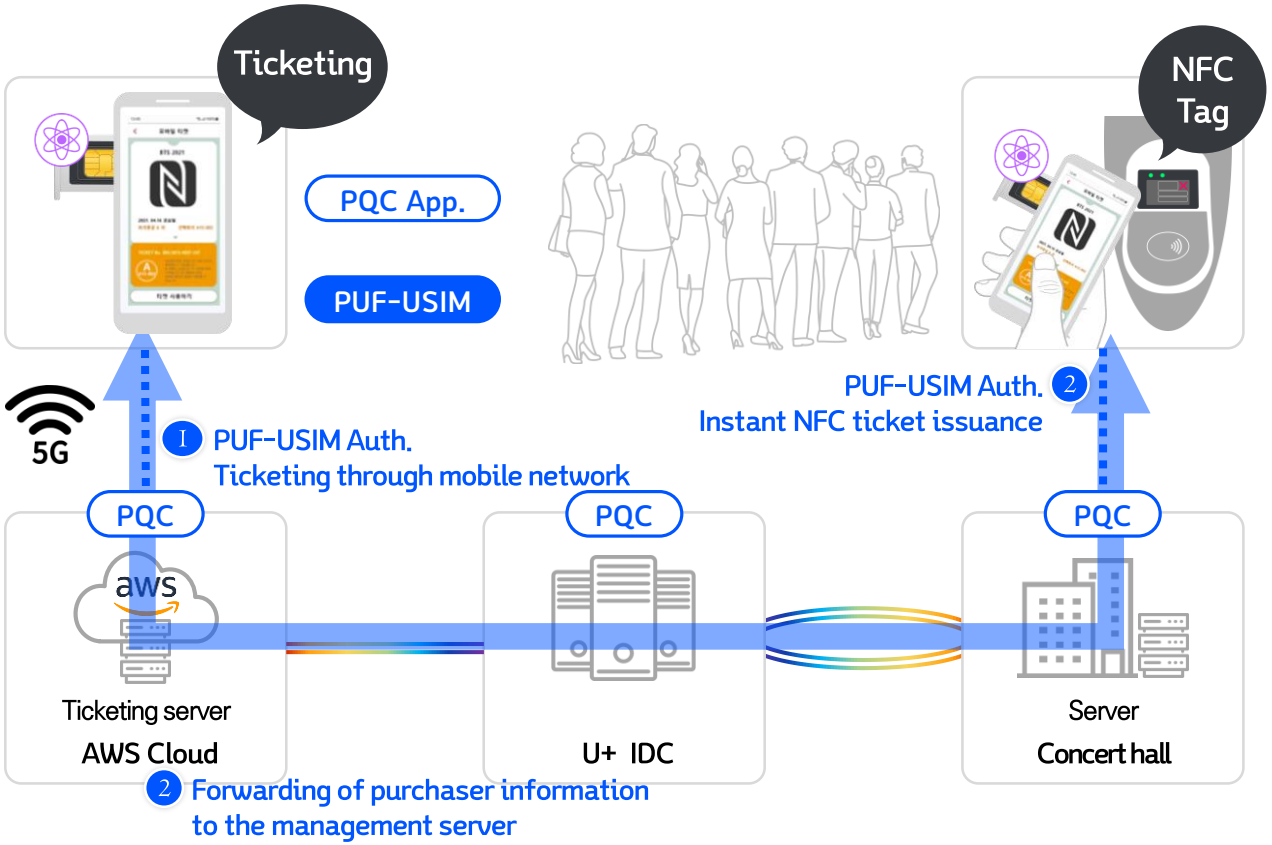
- QPUF User Auth. Log-in

- Factory database (open, upload, delete)



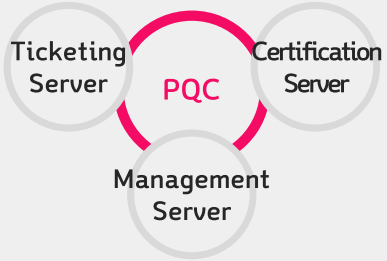
New application service with PQC applied – Culture industry

Performance ticket reservation service with PQC applied



Key points

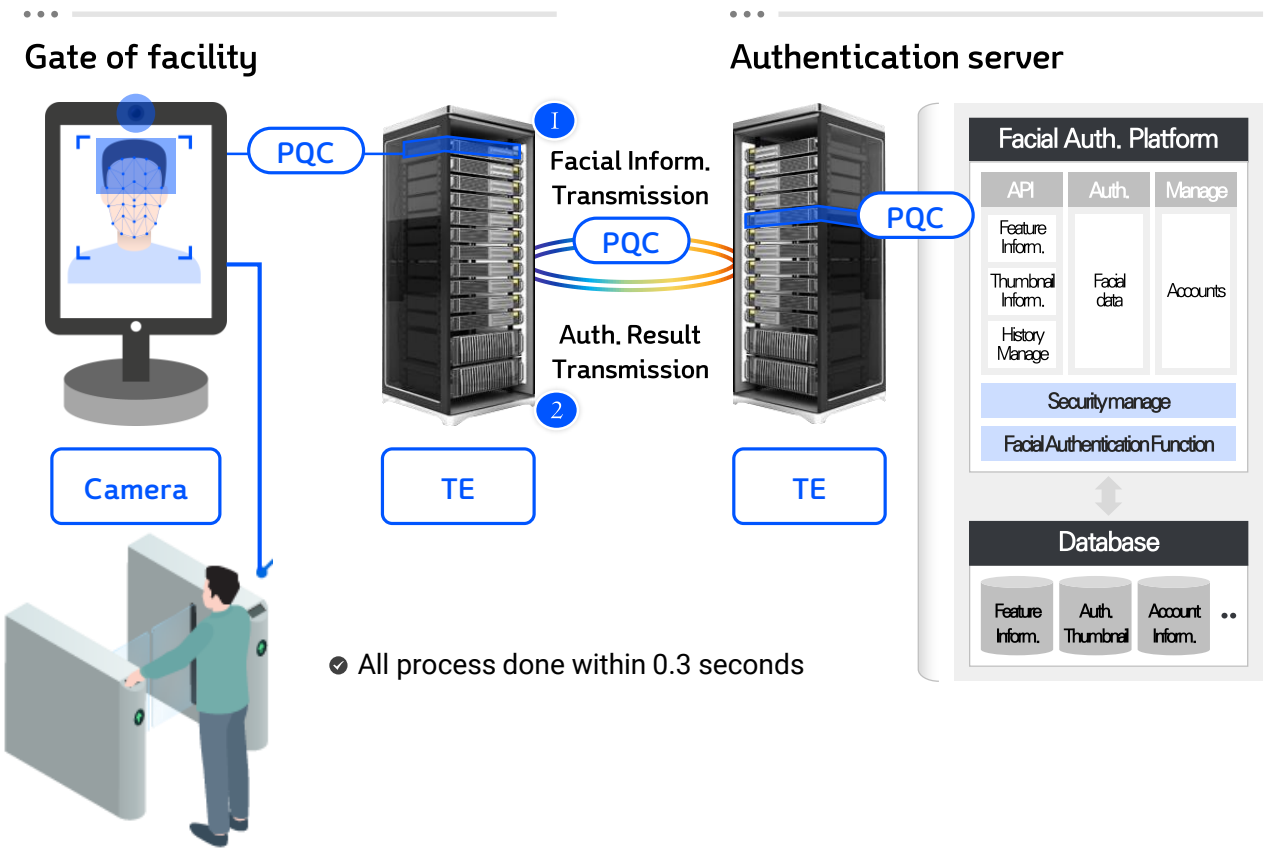
- Applying PQC to mobile applications
  - Wireless PQC service
  - PQC key exchange
  - PQC certification
- Applying PUF-USIM
  - Prevention of certificate theft



Sessions of all are PQC

New application service with PQC applied – Security facility

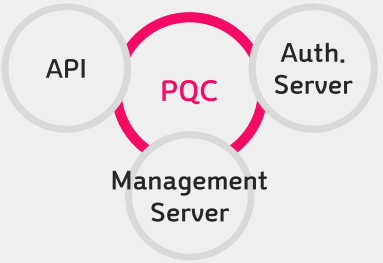
Facial recognition access system in security facilities with PQC



Key point

PQC applied to small Devices (Camera)

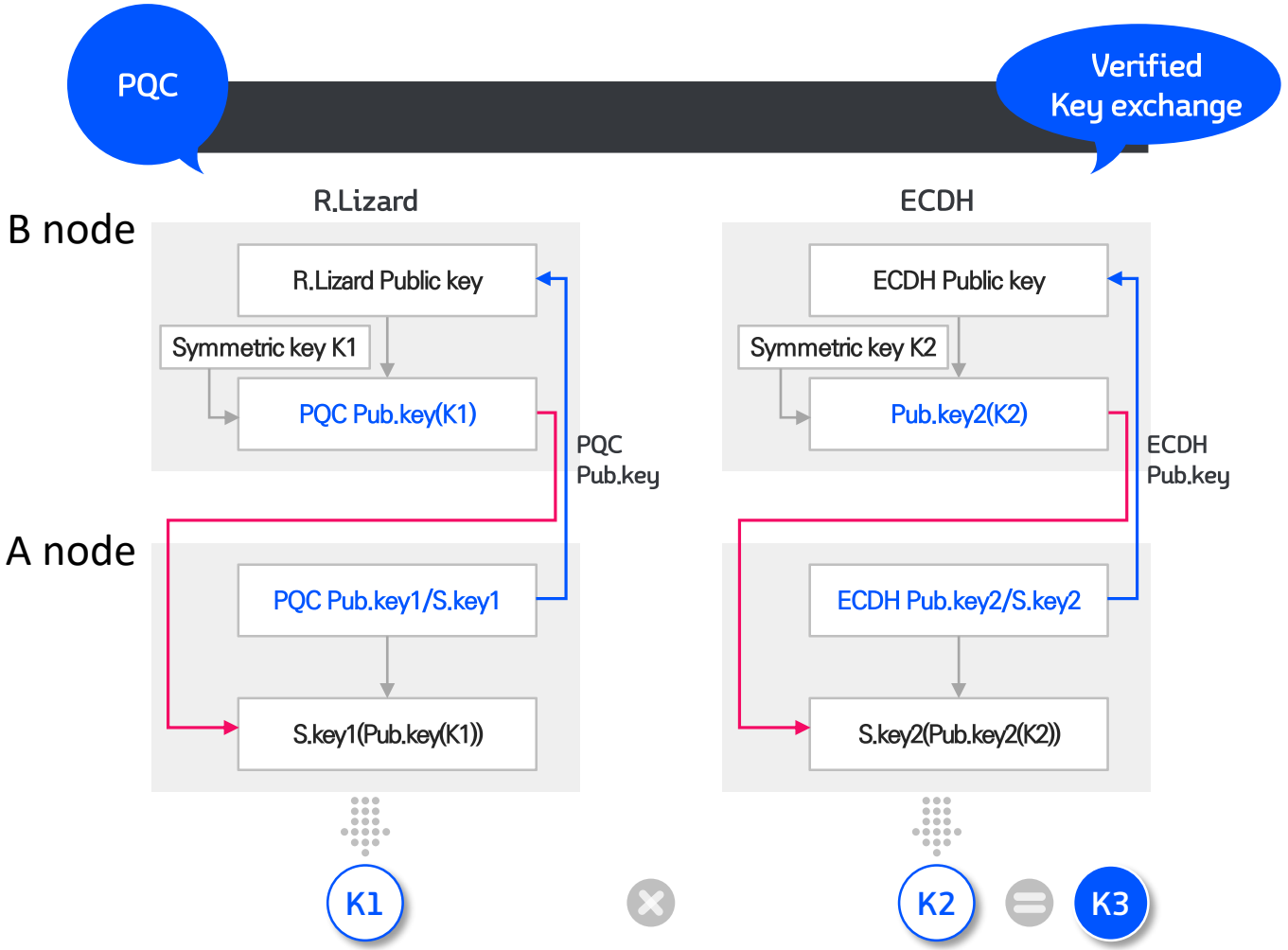
Apply PQC to the device so that access authentication information cannot be stolen



Sessions of all are PQC

Hybrid PQC algorithm – ECDH xor R.Lizard

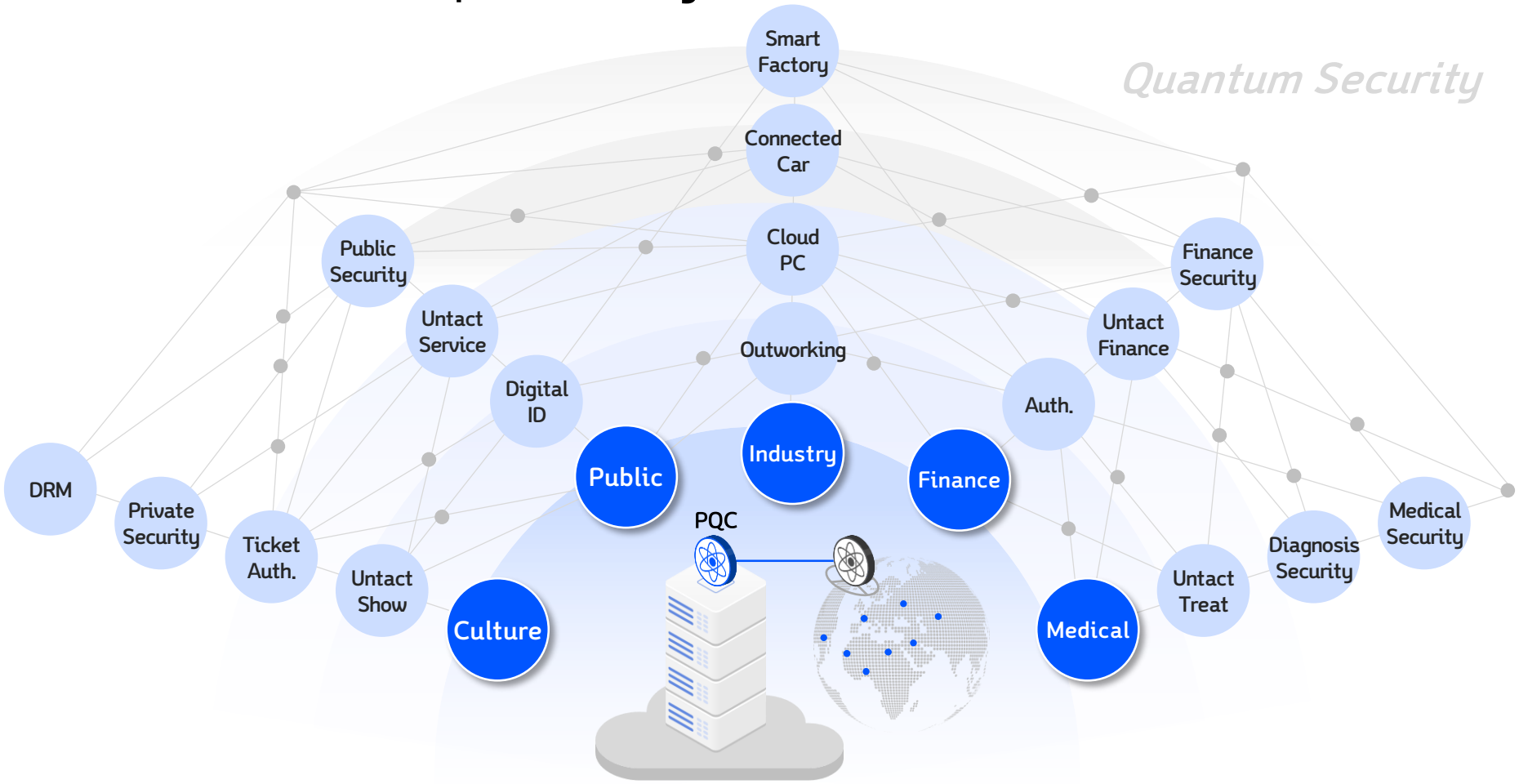
Securing stability through combination with legacy key exchange method



CHAPTER

IV Discussion and conclusion

LGUplus pursue a universal quantum cryptography platform that protects daily life of all our customers.



| PQC Platform |

Thank you for listening