National Institute of
Information and Communications Technology

Tokyo QKD Network and beyond

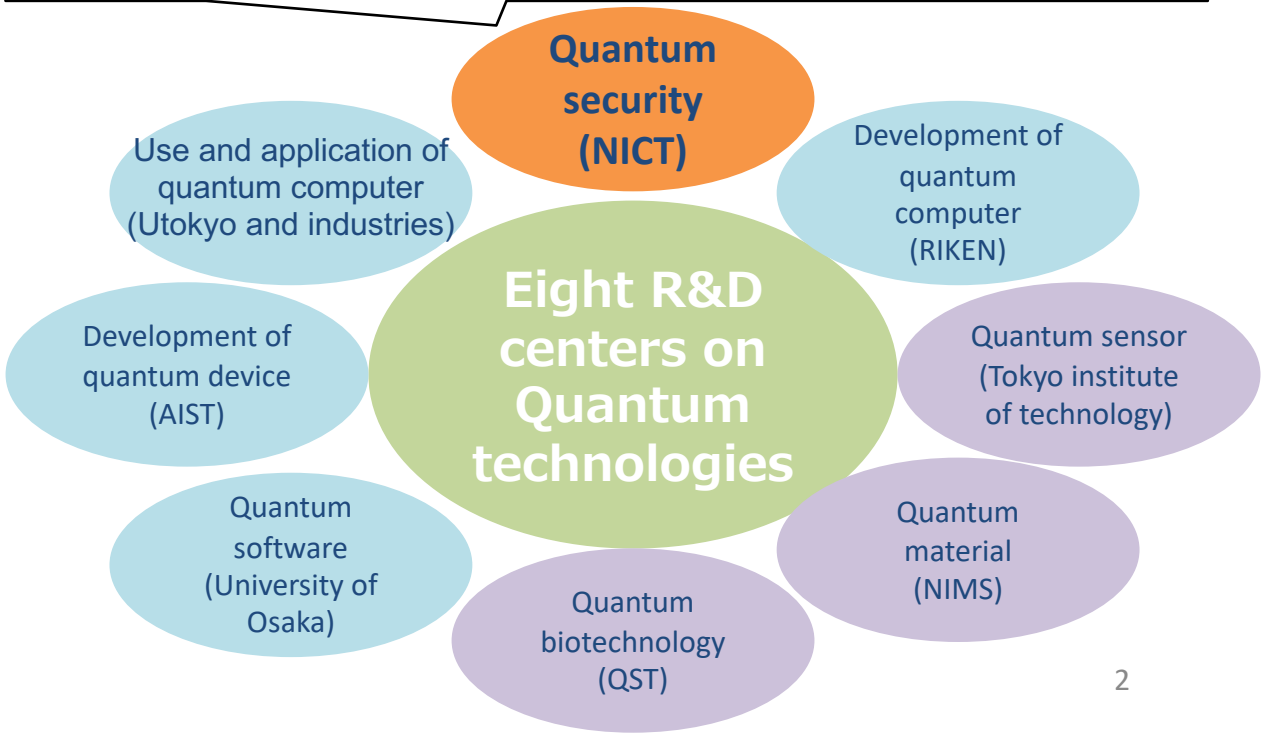
- How to leverage QKD over Open APN -

Quantum ICT collaboration center, NICT
Kaoru KENYOSHI
kaoru.kenyoshi@nict.go.jp

Quantum ICT collaboration center

- Eight R&D centers were established based on the Quantum Technologies Innovation Strategy to promote from basic research to implementation including developing of human resource.
- NICT established the **Quantum ICT collaboration center** as the core of eight centers for quantum security.
- **Quantum ICT collaboration center** is developing Tokyo QKD network and organizing feasibility testing of use cases such as quantum secure cloud collaborating with strategic partners.

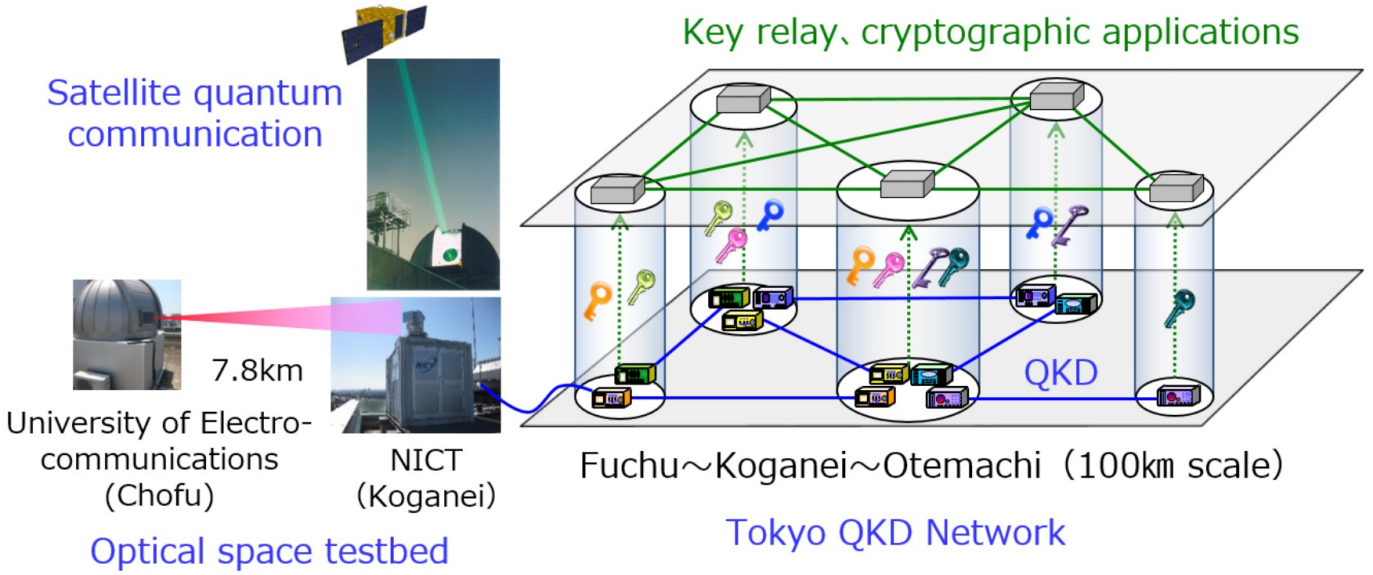
- Quantum ICT collaboration center was established in April 2021
- New building (Laboratory and Tokyo QKD network operation center) was launched in April 2022



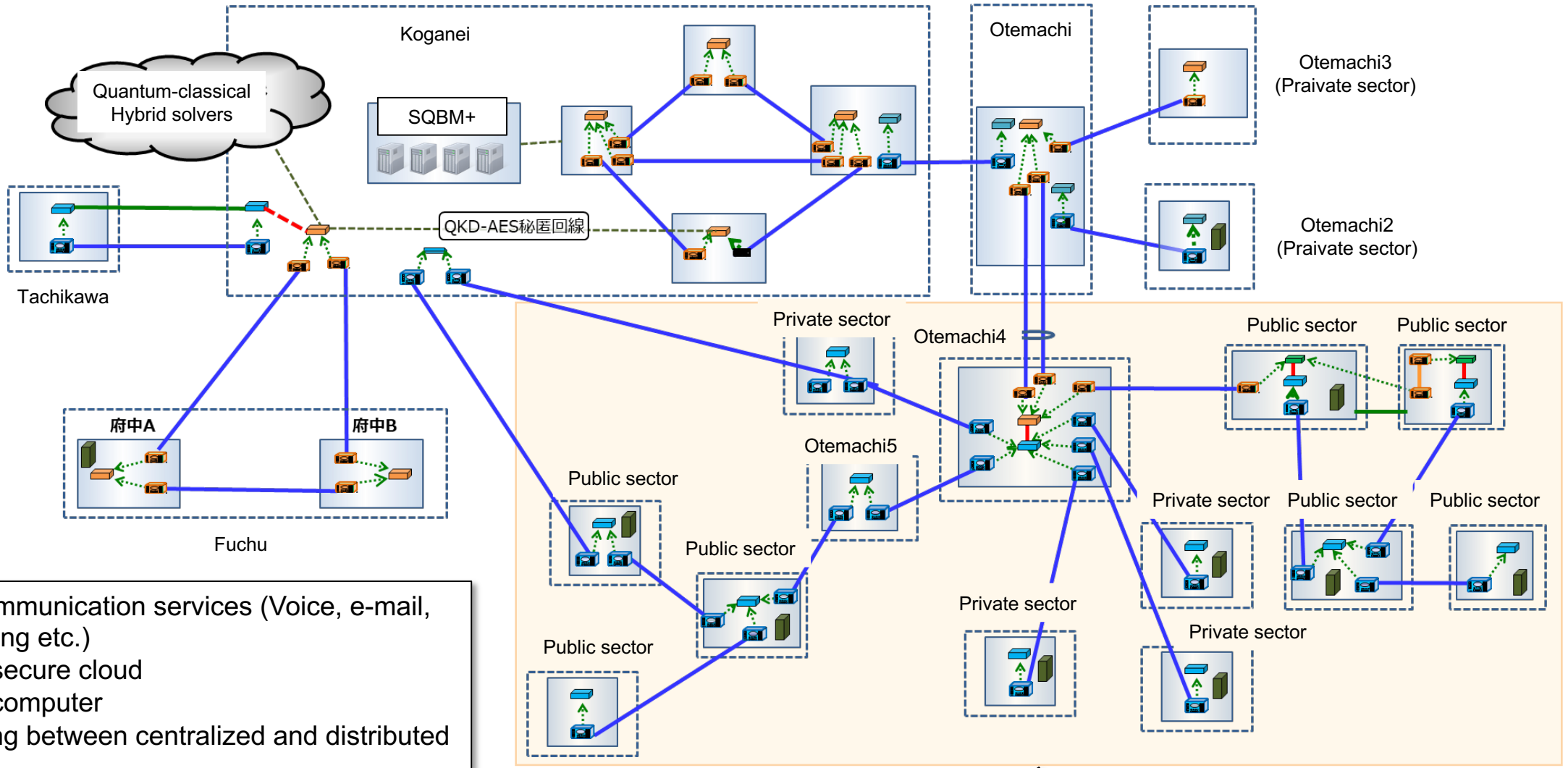
NICT: National Institute of Information and Communications Technology
AIST: National Institute of Advanced Industrial Science and Technology
NIMS: National Institute for material science
QST: National Institutes for Quantum and Radiological Science and Technology

Tokyo QKD Network since 2010

- QKD field testbed network on JGN-X in Tokyo, Japan
  - QKD links are connected via the trusted nodes
  - JGN: open testbed fiber network provided by NICT
- Constructed in 2010
  - World first TV conf. with quantum cryptography was demonstrated at UQCC2010)
  - 4 companies (NEC, Toshiba, MELCO, NTT), 8 universities, 2 national institutes (NICT, NII)
- Continuously operated for long-term field tests, enhancing network and developing applications.

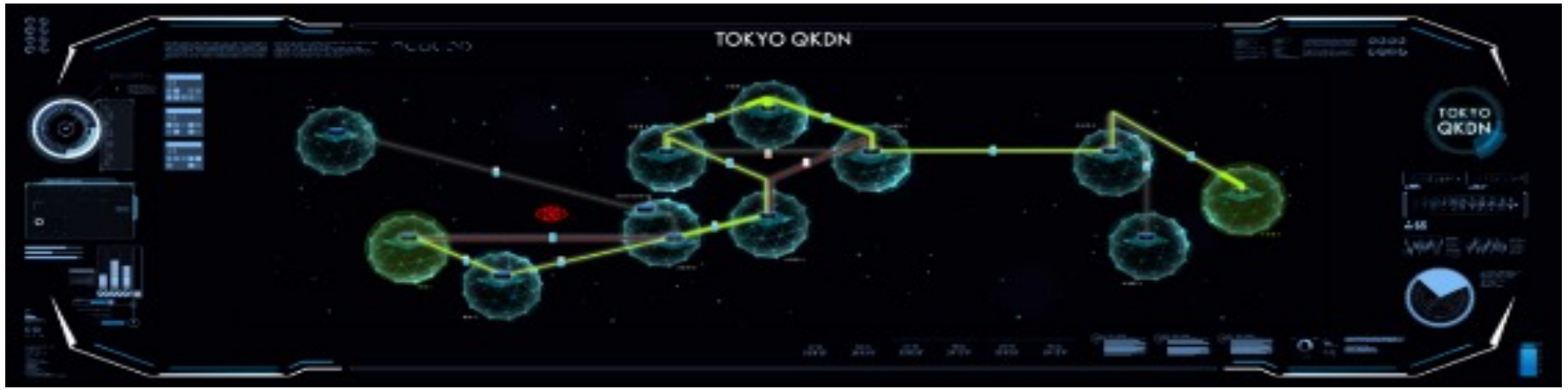


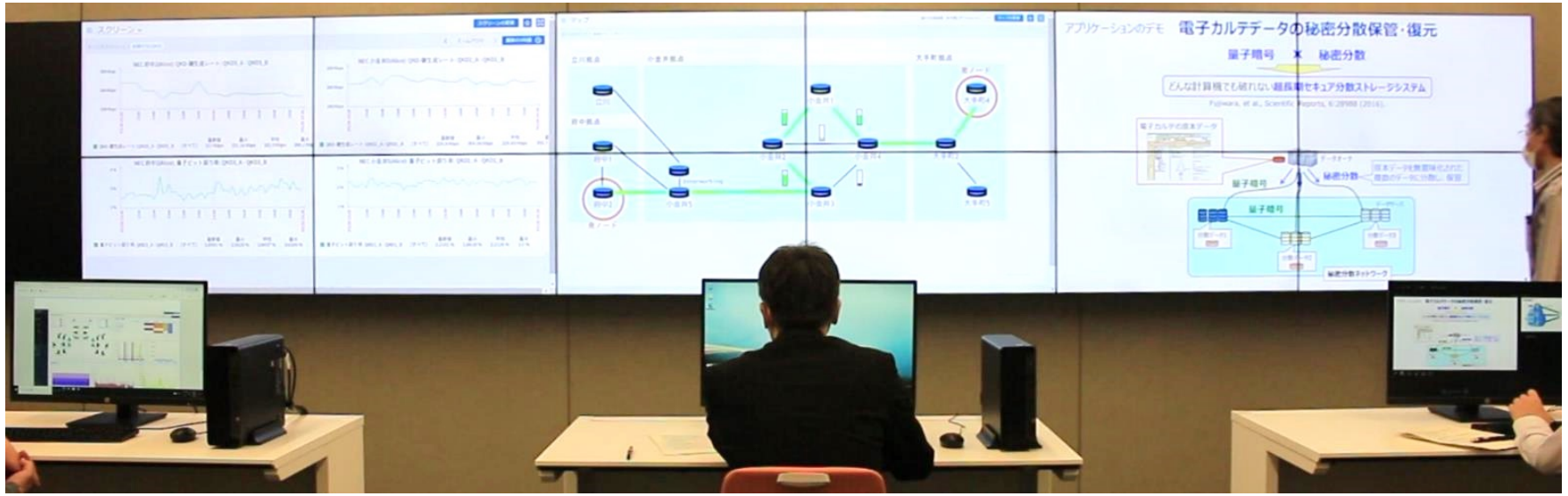
Tokyo QKD Network – Network structure -



- Secure communication services (Voice, e-mail, Web meeting etc.)
- Quantum secure cloud
- Quantum computer
- Interworking between centralized and distributed QKDNs

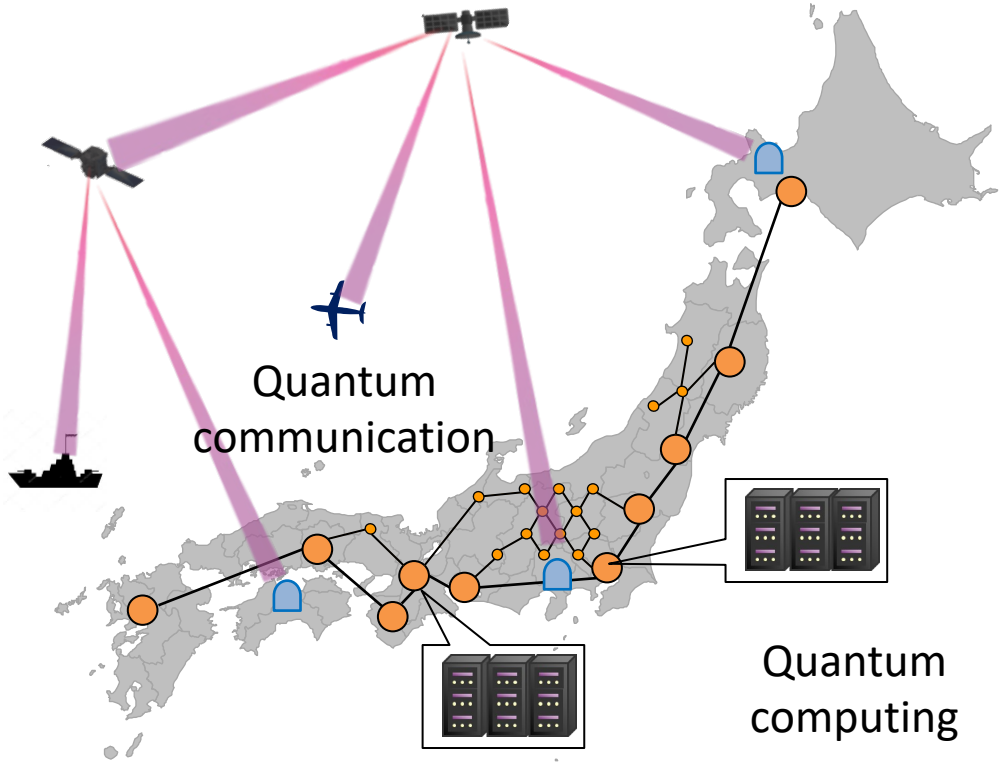
Tokyo QKD Network – Operation center -



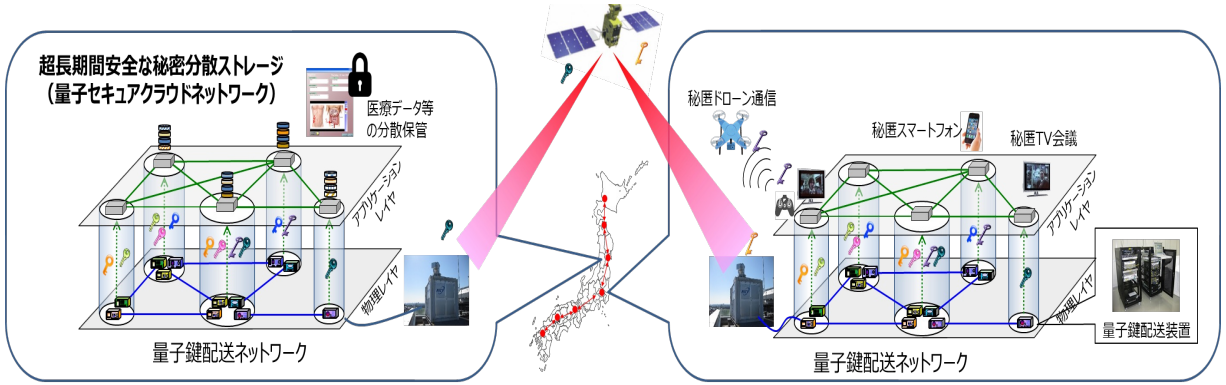


Tokyo QKD Network – Roadmap -

- ❑ Step 1 (～2023): Deploying Quantum Secure Cloud in the Kanto area
- ❑ Step 2 (～2025): Deploying Quantum Secure Cloud in each City
- ❑ Step 3 (～2030): Integration of satellite and terrestrial networks (all over Japan)
- ❑ Step 4 (～2035): Global Networking



satellite quantum cryptography



Integration of satellite and terrestrial networks

Tokyo QKD Network – Challenges -

- ❑ The current Tokyo QKDN implementation uses dark fibers which are provided by network operators to serve as a leased line between QKD modules.
  - ➢ In the future, the construction and deployment of QKDN will be easier if commercial communication services provided by network operators to support transmit quantum signal are available.
- ❑ The current demonstration of experiments are led by the government (government budget).
  - ➢ Commercial services led by private sectors are expected. In order for QKD service providers to provide them as commercial services, the investment cost for construction of QKDN should be lower. It is necessary to reduce the size and price of QKD modules and share the optical network.

For the development of QKDN in nation wide, we study the technical requirements for communicating quantum signal through the **IOWN APN** which will be the future network infrastructure.

IOWN GF presentation

Introduction of IOWN GF with several slides of “IOWN Global Forum Pitch Deck”

IOWNsec TF

IOWN security Task Force (IOWNsec TF) was established in December 2021 to study security aspect of IOWN.

Coordinator (primary contact point on the technical matters)

Kaoru KENYOSHI (NICT), kaoru.kenyoshi@nict.go.jp
Fumiaki KUDOH (NTT), fumiaki.kudoh.xr@hco.ntt.co.jp

Supporting Members

NICT, NTT, NEC, Toshiba, Red Hat, COMMSCOPE

Activities

IOWN security TF has developed the security reference document "**Technology Outlook of Information Security**" in 2022. We are going to develop the revision 2 of the reference document and PoC reference document in this year.

Technology Outlook of Information Security

Scope

This reference document identifies a reference model, analyzes security threats, defines security requirements and security levels, performs a gap analysis, and describes **Multi-Factor Security (MFS)** as a security measure. These descriptions are based on general procedures to study security measures, and It can be a reference to study details of security measures for IOWN architecture. It will achieve the following requirements:

- Protect and validate data communication between the endpoints for the entire communication lifecycle;
- Protect data stored in IOWN architecture for short-term and long-term;
- Protect data being processed in endpoints.

The first version of this document mainly focuses on the protect and validate data communicated between the endpoints.

Multi-Factor Security (MFS) architecture can combine multiple technologies to achieve end-to-end data protection with post quantum security. MFS could address a wider range of threats including sudden cryptographic compromise and achieve a required security level by the user that cannot be reached with a single method.

It was published in March 2023.

Scope

Table 1-1: Classification of information systems

	INFORMATION SECURITY	
	Protection of information	Protection of information systems
Definition in this document	Protection of user-generated data communicated or owned by users (including devices) of the IOWN.	Protection of the IOWN infrastructure itself.
Concrete examples	• Authentication of communication partners • Encryption of data • Exchange of encryption keys • Monitoring information	• IOWN management data protection • HW/SW protection • Supply chain security • Physical Security

NOTE 2 - The details of protection of information system is not described in this document. It will be described in future editions.

Reference model and threat analysis

For communication, this subsection refers to the high-level view and system model for communication. In the high-level view, end-to-end communication to be protected is described. The communication starts at communication endpoints, e.g., application processes, and continues to the other communication endpoints through the extra network and Open APN.

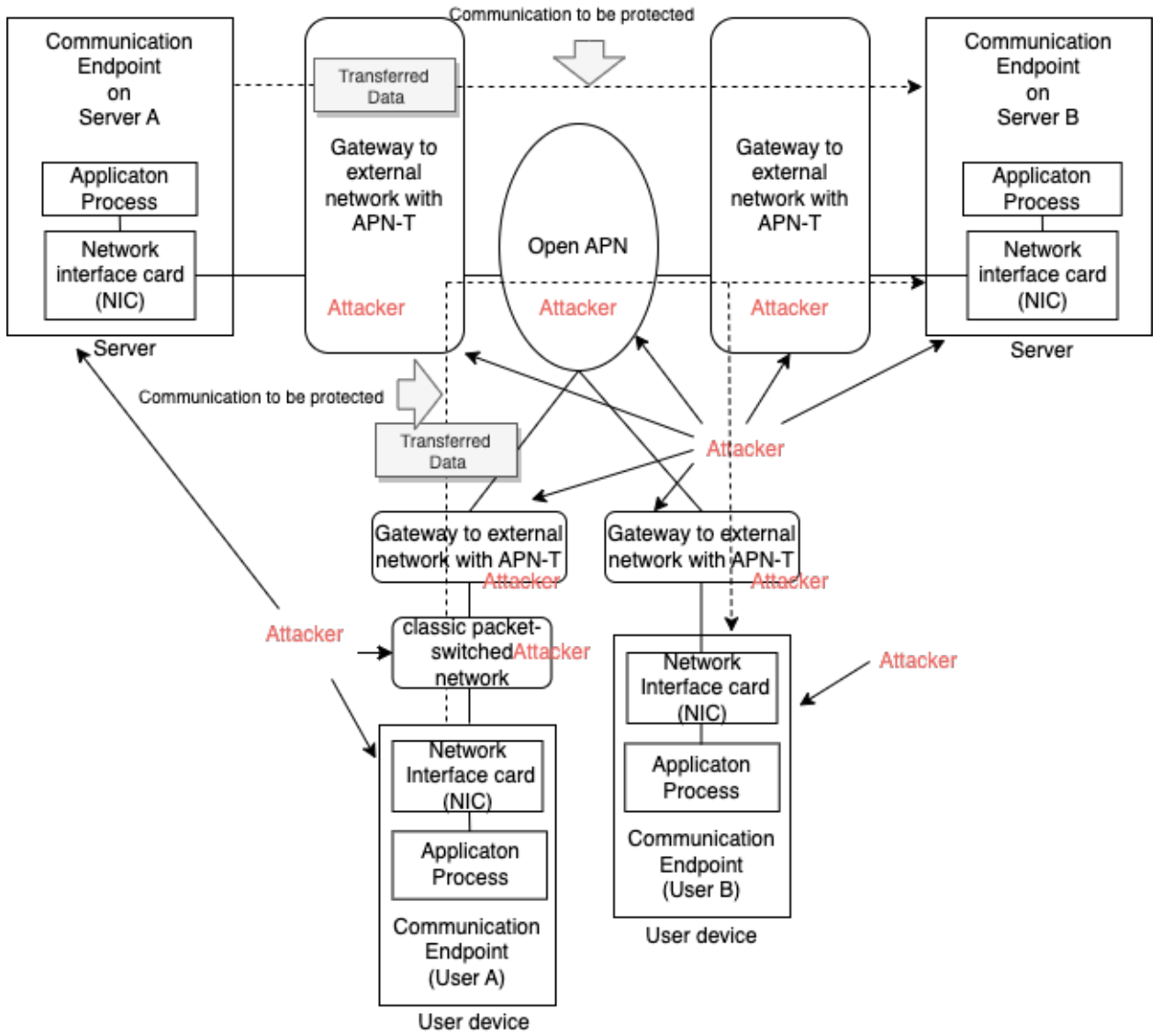


Figure 2.1-1: Reference model for communication

Security Requirements and Security Levels

Three data protection requirements that IOWN must satisfy are divided into the following three major categories.

- Protect and validate data communication between endpoints for the entire communication lifecycle (Data in motion);
- Protect data stored in IOWN for short-term and long-term periods (Data at rest);
- Protect data being processed in endpoints (Data in use).

The requirements for data protection are outlined in terms of the four security elements to be considered.

- Confidentiality
- Data integrity
- Availability
- Accountability

Of the above security elements, this version places particular emphasis on confidentiality and integrity.
The requirements for confidentiality and integrity, as well as the requirements for the security features themselves that IOWN should specifically consider, are detailed below.

1) Considering the threats from malicious insiders and dependence of third parties i.e., service providers and long-term data preservation;
2) Achieve the post-quantum security
3) Provide users with technology choices so that users can make a good balance between the cost and the security level
4) Without compromise the benefits of IOWN GF technologies, e.g., high capacity, low latency, and high energy efficiency

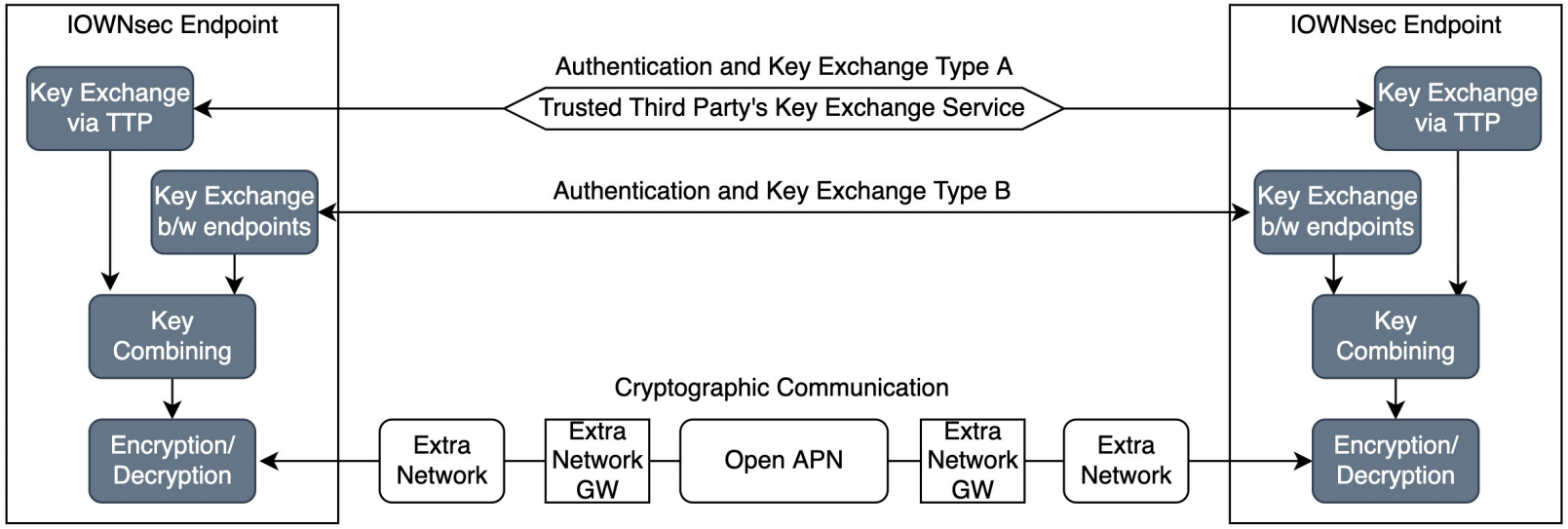
Direction for IOWNsec

What is Multi-Factor Security? (Basic Concept)

Multi-Factor Security (MFS) is defined as a technology that combines multiple security methods to achieve a security level that cannot be reached with a single method. A well-known example of MFS is multi-factor authentication (MFA) where different types of authentication factors are used in combination to counter different security threats.

Type A
Authentication and/or key exchange are supported by trusted third party.

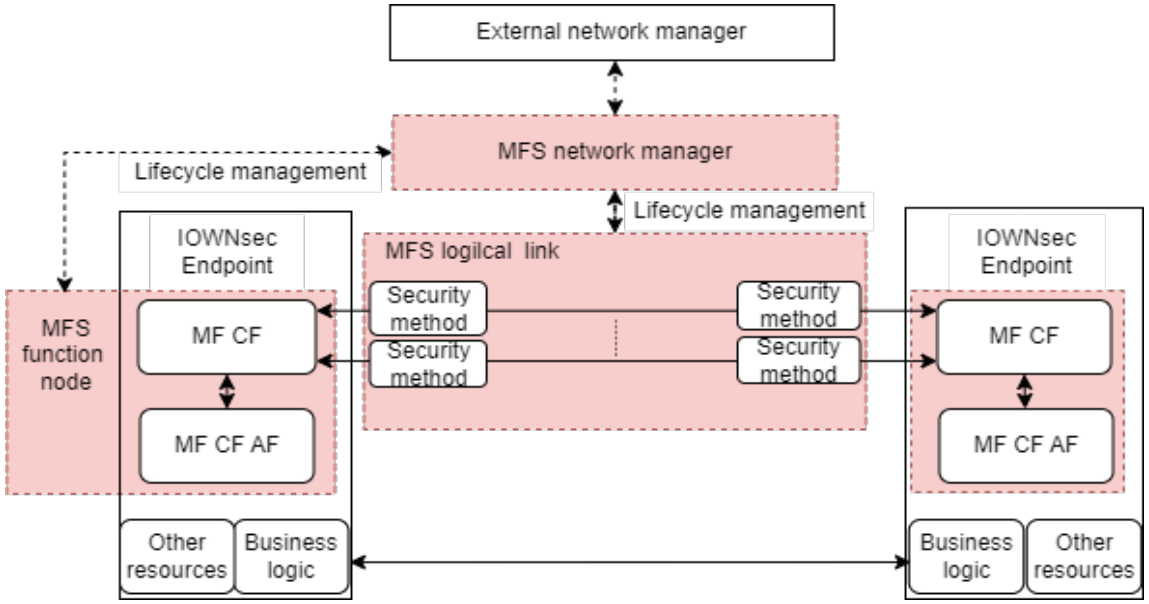
Type B
Authentication and/or key exchange are mutually supported by IOWNsec endpoints.



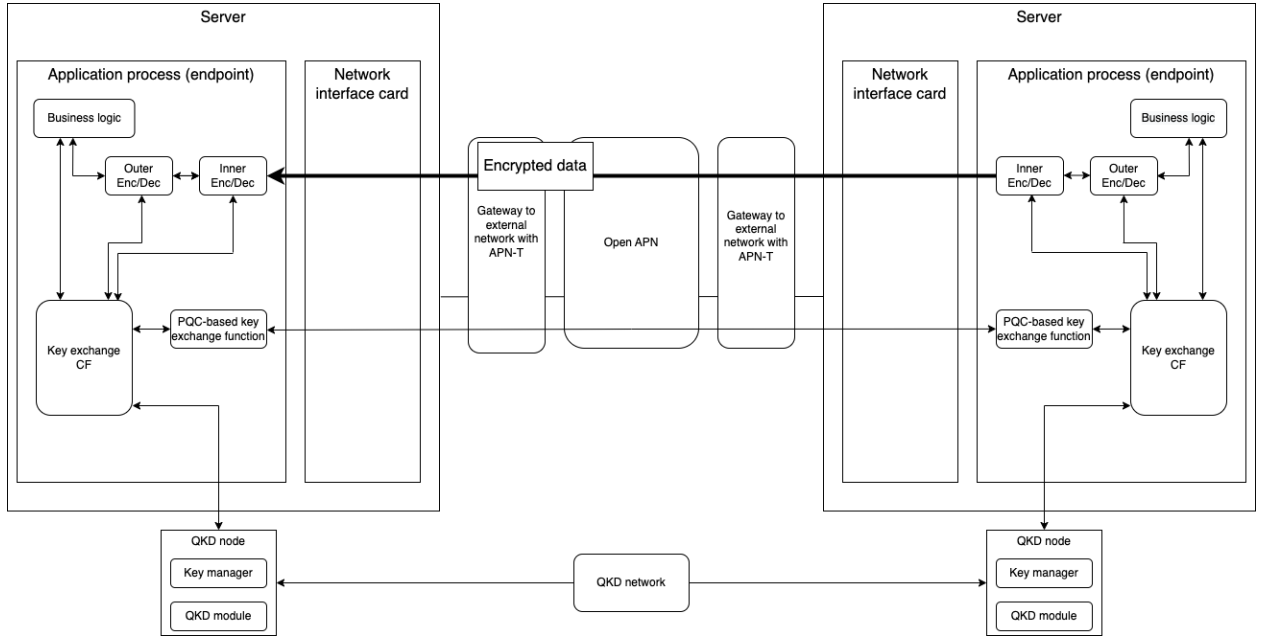
Specific example of multi-factor security

High level architecture and Examples

In this MFS scheme, multiple security methods are used to leverage the level of security. Multi-factor control function (MF CF) coordinates and controls these methods to satisfy the required security level. If additional functionality is needed in the process of MFS, MF CF adaptive function (AF) will perform these additional processes.



Multi factor security network architecture



Specific example of MFS system architecture for key exchange using QKD and PQC on endpoint

Conclusion of Rel.1

This reference document describes the security measures that can be taken against the security threats that increase with the advent of quantum computers. For IOWN to construct the next-generation social infrastructure, it is necessary to consider the security requirements from various users. By assuming attack points, and reviewing the information assets transferred, processed, and stored, it is possible to analyze security threats on them. After that, security measures that fulfill the security requirements of users are examined. All security measures have pros and cons, and it is difficult to satisfy the various security levels required by users alone. It is realistic way to introduce MFS that combines multiple security measures. This reference document describes the MFS architecture that IOWN should implement.

The first version of the reference document provides an overview of IOWN security and focuses on protection of information and communication. Other aspects of security such as protection of information system and protection of data store, etc. will be described in the future revisions.

Current WIs of IOWNsec

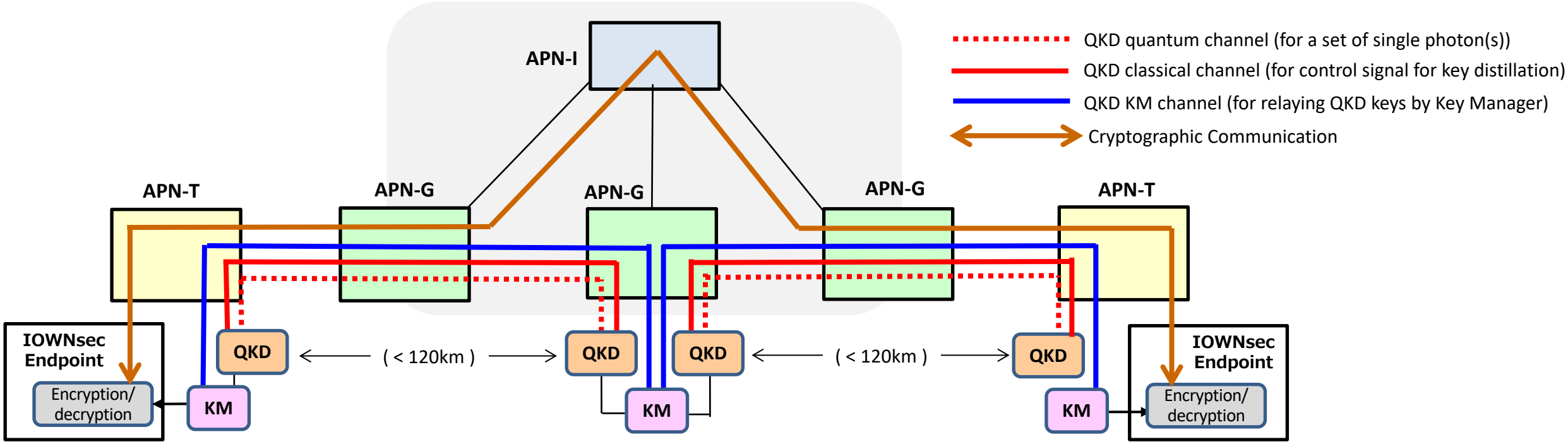
IOWNsec TF is developing the Release 2 reference document on the following four topics and made progress on them.

- Zero-trust security in IGF architecture
- MFS enhancements
- **QKD over Open APN**
- SEC-PEC Collaborative Architecture
- Direction of SEC-DCI collaboration
- PoC reference document

Implementation Example (as a case study)

In order for a set of single photon(s) to be transmitted between neighboring QKD devices (quantum channel ·····),

- QKD devices, where single photon(s) are terminated, should be able to be attached to APN-Ts and APN-Gs
- Fiber cross-connect functionality which is provided at APN-G without amplifier should be okay for single photon(s) transmission.



Conclusion

- IOWN APN supports future network infrastructures. It is an all-photonics network introduces photonics (optical) - based technology into all components from networks to terminals. This technology is essentially compatible with end-to-end quantum communication. We study the technical requriemetns to support transmitting of quamtum signal through IOWN APN.
- MFS architecture is a combination of multiple security technologies to achieve end-to-end data protection with post quantum security. PQC and QKD can be incorporated into the IOWN APN and support various level of security.