IOWN GLOBAL FORUM ™

Technology Outlook of Information Security

Classification: REFERENCE DOCUMENT

Confidentiality: PUBLIC

Version 1.0

[SEC]

Legal

Contents

List of Figures

List of Tables

1. Introduction

1.1. Objectives

Security for IOWN communication and storage is vital to support future ICT infrastructure. In recent years, quantum computers have made remarkable progress toward practical use, and complex calculations that were previously impossible become solvable. In addition, it has been pointed out that public key cryptography such as RSA and elliptic curve cryptography, which are used in various aspects of the current ICT society, can be compromised in a realistic time by using quantum computers. In order to secure transferring and storing data of IOWN architecture, appropriate security solutions are required against threats which are derived by quantum computers.

Due to the appearance of new security threats like the emergence of quantum computing, some changes in the security model or security trends are taking place. In today's network, it is recognized to be difficult to protect all the cyberattacks from outside attackers completely. In addition, cyberattacks from inside the organization should be considered at the same time. Based on the thought that perimeter-based security defense model is not enough for today's security environment, or that the inside of a network is no more secure, the idea of "Zero Trust" has been widely spread. C.f. [NIST SP-800 207].

Additionally, the notion of "as a service" became popular in recent years. When subscribing to a third party's service, a user will depend on them much more in terms of functional or nonfunctional aspects. In a cloud security framework, a shared responsibility model dictates that the cloud users depend on the cloud providers to ensure accountability. Vendor lock-in/lock-out is also very important considerations.

This reference document was developed as a framework for describing the security of IOWN GF. Each TF of IOWN GF studies the details of each security, and this document is expected to be the umbrella document of them.

1.2. 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.

To achieve the above, there are some supplemental requirements,

- Consideration of the threats from malicious insiders, dependence on third parties i.e., service providers and long-term data preservation;
- Achieve the post-quantum security;
- Provide users with technology choices so that users can make a good balance between the cost and the security level;

- Without compromising the benefits of IOWN technologies, e.g., high capacity, low latency, and high energy efficiency.

NOTE 1 - The details of commonly discussed technical aspects such as the protection of personal information, handling of privacy, security risks and measures for hardware and software are outside the scope of this document.

ITU-T and NIST Special Publication 800-12 defines information security as follows.

Information Security – Preservation of confidentiality, integrity and availability of information. [ITU-T Y.3500]

-Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. [NIST SP800-12]

Information – (1) Facts or ideas, which can be represented (encoded) as various forms of data; (2) Knowledge (e.g., data, instructions) in any medium or form that can be communicated between system entities. [NIST SP800-12]

This document defines and classifies information security as follows.

This version focuses on the protection of information in the following categories.

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.

2. Reference Model and Threat Analysis

2.1. Reference Model for Information Security

This subsection describes the reference models for communication and data stored in storage.

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.

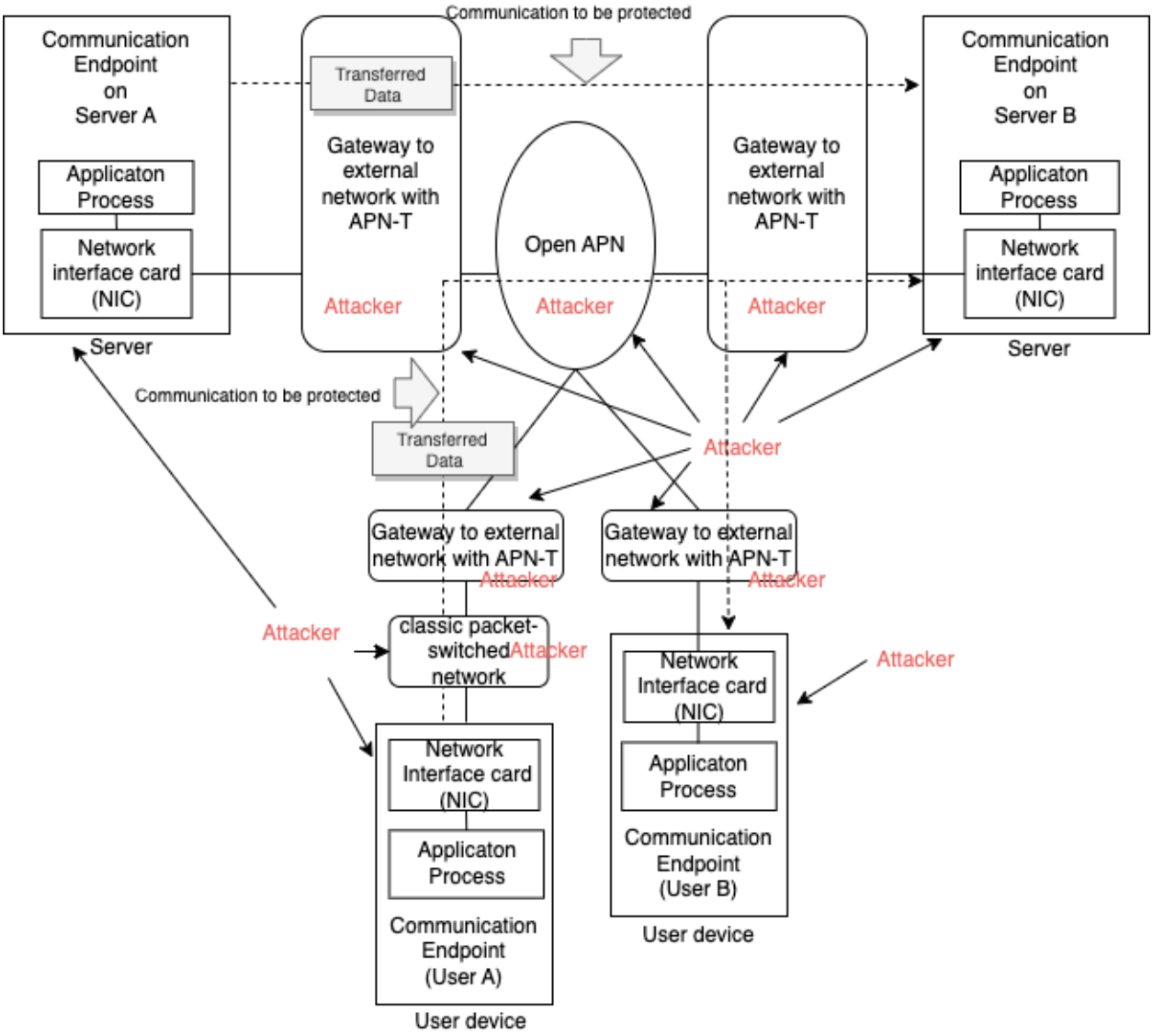

Figure 2.1-1: Reference model for communication

- Open APN

The Open All-Photonic Network (APN) is a network that connects endpoints directly with optical paths. It provides high-speed, ultra-reliable, and low-latency connections. In today's network, optical paths are disjoined and operated on a segment-by-segment basis. By contrast, the Open APN will enable one optical path to span across multiple segments. This will enable end-to-end communication with deterministic performance.

- Communication Endpoint

Exact definition of "Endpoint" in IOWNsec is the point where protected data are generated, processed, or consumed. Generally, "endpoint" will be application processes within an end node.

There can be two major end nodes in this document: customer premise user devices and servers on a network. The scope of the end node may vary depending on the implementation and its security level. For example, it could indicate a single server, or it could indicate a specific server room or a specific location.

In either case, there are two possible forms of end nodes. One is connected to the extra network and the other is directly connected to OpenAPN.

In the context of channel encryption, the term "endpoint" is usually recognized as the point where protected data are sent or received, but when considering end-to-end data protection, the "endpoint" should be the exact definition above the application process.

If processes or devices independent of the endpoint are secured at the same level of the application processes that are the endpoints, some implementers may choose to implement encryption functions in such an embedded process and device (hereinafter referred to as "near-endpoint") instead of endpoints. IOWNsec should allow such implementations. However, the security level of such implementations depends on the security level of the execution environment containing the application process and the encryption function. Measures for the protection of this environment are outside the scope of this version of IOWNsec. Given that, it is important to note that the security level of systems that rely on near-endpoint encryption functions depends on implementations. And it should be noted that in many cases the near-endpoint is owned by a third party.

Such "near-endpoint" can include devices and processes which are embedded on the devices.

For example, CPS/AIC use case workloads include an image analysis process and TLS encryption/decryption service to protect data transfer, and these two workloads work together in a single node. The former is considered an endpoint, and the latter is considered a near-endpoint. Another example is a mobile device which has a single application where the device's security is almost same as the application process.

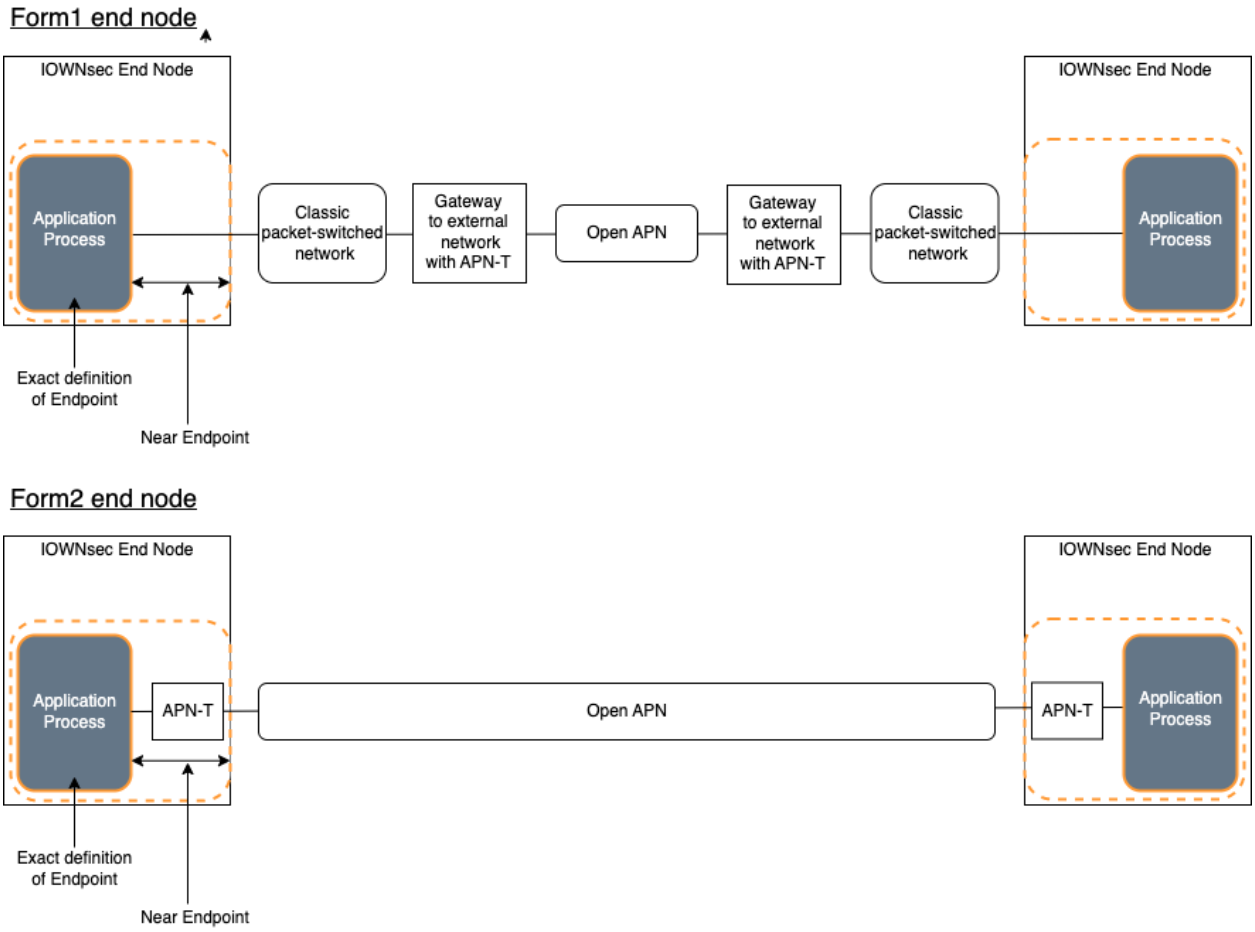

Figure 2.1-2: Definition of Endpoint

Figure 2.1-3 refers high-level view and system model for storage. In high-level view, data are put into or got from an endpoint, e.g., application processes that provide or consume the data.

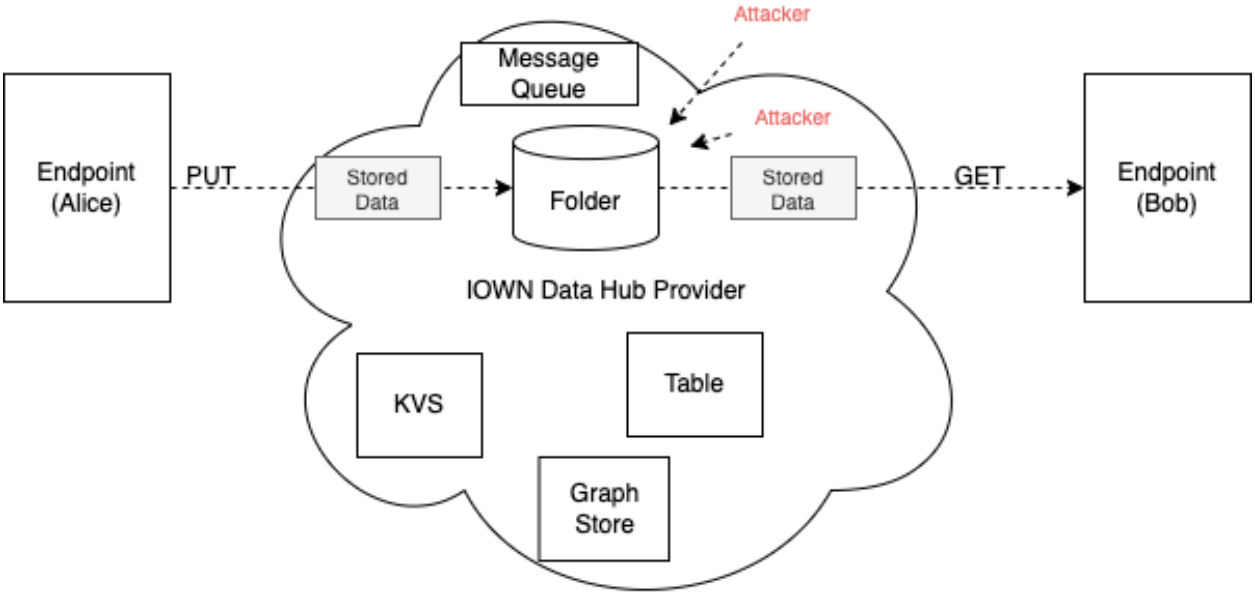

Figure 2.1-3: Reference model for storage

Taken together, there are three main categories of locations where data should be protected as shown in Figure 2.1-4.

- Data in motion

  Data in motion is data in transit between IOWNsec endpoints or within computer systems.

- Data at rest

  Data at rest is data that is neither in use nor in motion (i.e., being located at some storage).

- Data in use

  Data in use is data that is currently being processed by IOWNsec endpoints.

Of the above, this document focuses on data in motion.

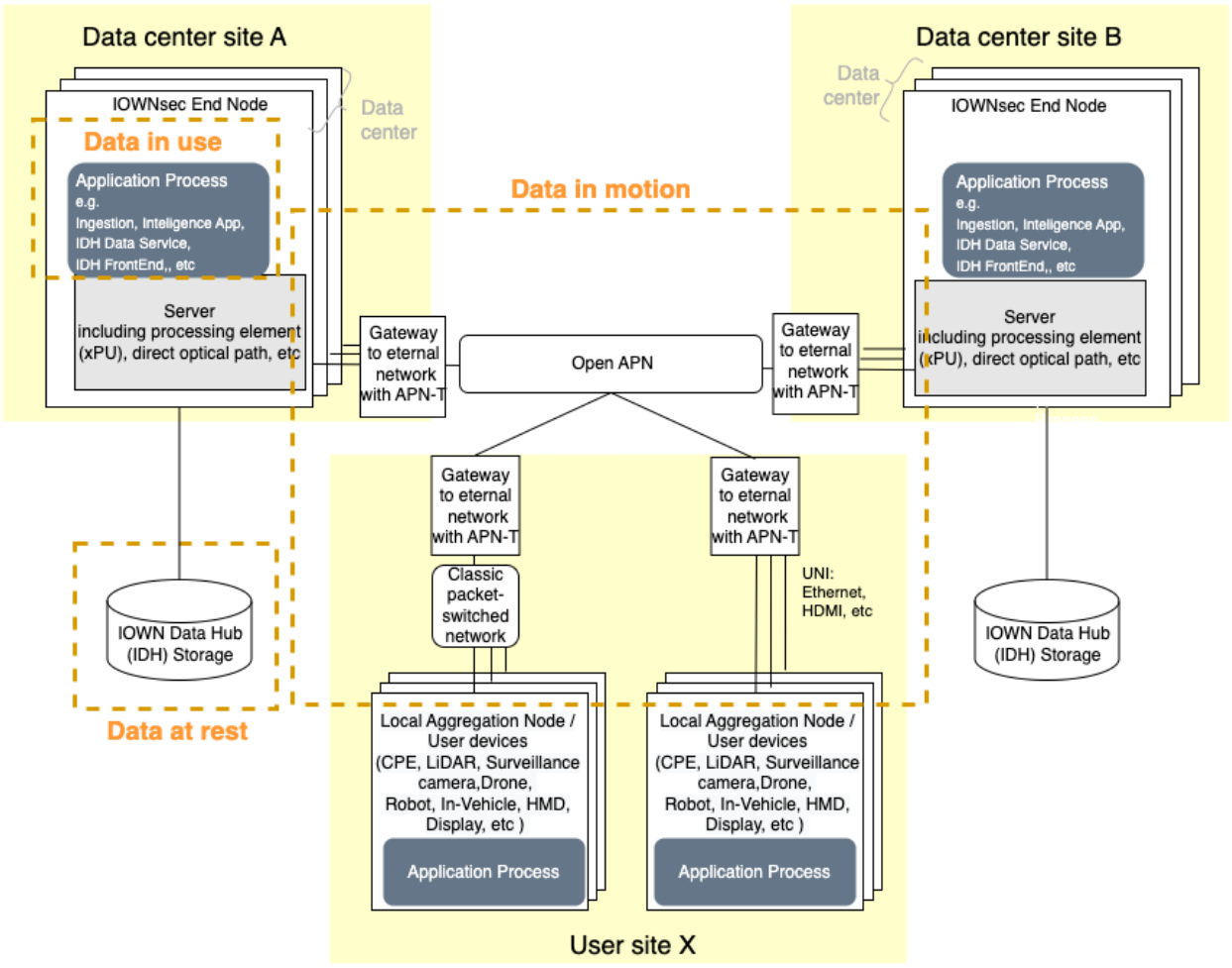

Figure 2.1-4: Categories of data should be protected

This version does not include a detailed threat analysis of the systems included in the reference model. This version focuses on authentication and encryption as common data protection security for E2E communication of the reference model.

2.2. Information Assets to be Protected

This version does not include a security analysis of IOWN GF architecture or specific data to be protected, but rather provides an overview of threats in E2E communication at the level of abstraction of the reference model in section 2.1. As an example of concrete assets to be protected, reference implementation model considered in IOWN GF can be referred to. The information assets to be protected in IOWN GF CPS RIM are listed in Appendix A as a reference.

2.3. Security Threats

With the advent of quantum computing, the incorporation of the Zero Trust model from perimeter-based security defense models, third-party service reliance, intrusion from supply chain weaknesses, … threats to systems will be ubiquitous, therefore IOWN GF need a multifaceted view of the threat.

In order to protect the information assets in a quantum computing era, it is necessary to take countermeasures with stronger encryption. In addition, it is necessary to recognize threats based on the idea of zero trust security.

This version focuses on authentication and encryption as a common data protection security for E2E communication path of the reference model.

This version present risk mitigating method by authentication and encryption as countermeasures against many threats. Threats that can be mitigated by authentication and encryption are both external and internal threats in the attack points in Figure 2.1-1. For future study, the Appendix B shows the position of "this version" in the general threat list.

2.3.1. Security Threat Overview

[STRIDE], [MITRE AT&CK], and others are known as threat analysis for real systems and organizations where the environment and configuration are known. However, it is difficult to apply them in IOWNGF, which does not identify real systems or organizations.

Instead of using the approach of planning countermeasures from threat analysis, this version shows threats that can be mitigated by authentication and encryption. Therefore, this section organizes the threats that can be mitigated by authentication and encryption in STRIDE's model.

Spoofing:

Threats that cause application malfunctions from Network interface card of servers or user devices by inputting information into the system may be based on information that a malicious third party used the power of quantum computers to infiltrate the internal network or bribed and infiltrated the system administrator, masquerading as a legitimate.

Tampering:

Collect information about third-party servicers and supply chains by monitoring Gateway to external network with APN-T or Open APN, comprehensively utilize the power of quantum computing to perform AI analysis and intrusion, and falsify notification messages and instructions to police/security personnel. As a result, threats may cause great damage to society, such as assisting in murder.

Repudiation:

Malicious third parties or internal criminals modify the video streaming data of surveillance cameras in the Folder in reference model for storage, Repudiation threats include unauthorized modification or destruction of data and could destroy surveyed evidence.

Information disclosure:

Threats related to information disclosure occur when systems such as servers and user devices are intruded by malicious third parties or internal criminals and data is stolen, as described in the example above. In addition, we assume threats that there are cases where physical branches are inserted into communication channels, real-time communication data is stolen, and decoding it over time with the power of quantum computers. When using a third-party service, information disclosure from internal criminals of the third-party service is also a possible risk.

Denial of Service:

By illegally generating large number of requests to create the keys required for encrypted transfer of video streaming data at Communication Endpoint, this is the case when creating a situation that exceeds IOWN architecture's key generation capacity, making encrypted communication impossible, it is a threat that is hindering and may even stop/break the service.

Elevation of privilege:

After trespassing to on the Open APN using quantum computer power, tampering log and leaving a program that can be executed.

When log analysis is performed under a privileged account, the corresponding program is executed under a privileged account, we assume threats that program cause upsets the load balance of the APN, causes long-term network communication failure, and causes a great loss to society.

3. Security Requirements and Security Levels

3.1. IOWN Security Requirements

This section describes data protection requirements that should be specifically considered in the IOWN era and does not represent a complete list of security requirements.

It is assumed that users have several levels of requirements for security according to their specific communications and data architectures. Several technologies can be considered to fulfill various aspects of these security requirements.

Three major categories for data protection

As described in Section 2, the 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).

This version describes the requirements for “Protect and validate data communication between endpoints for the entire communication lifecycle”.

In terms of security elements

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

- **Confidentiality**

IOWN should ensure the confidentiality of transferred data between the endpoints defined in section 2.1.

Information of user data should not be available to unauthorized parties for a sufficiently long period of time specified by users.

Based on a zero-trust approach, user data should be protected in all communications, regardless of network location, considering the risk to insiders including those of third parties (e.g., service providers).

When user data is transferred via a link in the IOWN architecture, the user data should be protected by the appropriate security measures such as encryption of the data and authentication of communication parties.

- **Data integrity**

IOWN should protect the integrity of stored and transferred data.

The data integrity functions provide the means to ensure the correctness of transferred data, protecting against modification, deletion, creation (insertion) and replace of exchanged data. For user data, integrity should be protected in transfer until delivered to the user or consumed by the user.

In most cases, cryptographic algorithms with appropriate computational security can be used. Post-quantum cryptographic techniques should be employed in accordance with their standardizations and practical deployments. In addition, IT-secure methods (e.g., Wegman-Carter message authentication) can be employed to protect the integrity of the information for data transfer.

- **Availability**

IOWN architecture should ensure the availability of its operation.

Security measures to support capability are:

- Redundancy of system such as 1: 1 or 1: n protection;
- Detour routes for data transferring.

IOWN architecture should have capabilities for network resilience.

Network resilience is the ability of the network to adapt to and recover from situation changes, including disruption, to continue acceptable levels of service in the face of security threats.

If security incidents are detected, the network resilience capability ensures they are handled in a controlled way, minimizing the damage caused. In addition, it ensures recovery of the system, restoring it at the required security level.

IOWN architecture should implement counter-measures against DoS attacks.

For example, network performance may be reduced (even to zero) due to DoS attacks on links. This issue could be mitigated by appropriate methods, including switching to backup links and rerouting of data transfer.

- **Accountability**

IOWN architecture should ensure that records of security critical actions are traceable uniquely to functional elements that performed the actions.

IOWN architecture should support traceability of data.

These two security requirements are supported by the dual functions of activity logging and security audits. Another possible but potentially weaker realization of accountability is achieved by the appropriate combinations of the authentication, access control, and audit trail functions.

IOWN architecture should have the capability of storing information activities relevant to security in the IOWN architecture.

IOWN architecture should generate alarm notifications on security events. The security alarm notifications are information regarding operations pertaining to security.

IOWN architecture should have capability to analyze logged data on security events.

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 architecture should specifically consider, are detailed below.

(1) Considering the threats from malicious insiders and dependence of third parties i.e., service providers;

Based on a zero-trust approach, user data must be protected in all communications, regardless of network location. In addition to external attackers, internal attackers at any location must be anticipated and the protected communications data must be encrypted between endpoints. The use of third-party services must also consider the risk of attackers inside the third-party service, regardless of whether the third-party service itself is malicious or not.

(2) Achieve the post-quantum security

It has been pointed out that public key cryptography, which is used in various aspects of today's ICT society, may be deciphered in a realistic amount of time using quantum computers. To maintain the security of IOWN over the long

term, IOWN architecture needs to provide a means by which user data can be protected from attacks that utilize quantum computers.

At the same time, security against existing threats must not be compromised. Furthermore, we must be prepared for new threats to cryptographic algorithms, since we do not know when and if new cryptographic algorithms will be discovered to be vulnerable. In other words, it is desirable to increase “crypto-agility”, which is the ability of crypto systems to respond quickly and flexibly to new threats, to prepare for possible future threats of cryptographic compromise.

(3) Provide users with technology choices so that users can make a good balance between the cost and the security level

Since various security levels are assumed for the services realized by IOWN architecture, it is difficult to uniformly specify security measures and strengths. Therefore, it is necessary to be able to flexibly select the means and strength of data protection depending on the service to maintain a balance between system security and cost.

The ability to have multiple security measures and to switch between them easily is also an important requirement to respond quickly to new threats to data protection that may appear in the future.

(4) Without compromise the benefits of IOWN GF technologies, e.g., high capacity, low latency, and high energy efficiency

It is necessary to ensure that the security features do not interfere with the various performance requirements that the IOWN infrastructure is trying to achieve.

Sections 3.1 and 3.2 define the evaluation measures for evaluating the security level of security methods in the IOWN architecture based on the above requirements.

3.2. Security against Computational Attacks

These security levels define the security against cryptanalysis in security measures utilizing cryptography.

Level 1 Traditional Computational Security: Maintains security against **known** attacks that are implementable with traditional computers

Level 2 Post-Quantum Computational Security: Maintains security against **knowns** attacks that leverage quantum computers.

Level 3 Information-Theoretic Security: Can theoretically prove that it is **impossible** for a third party to decrypt the exchanged data or recover the secret keys.

3.3. Security against Third Party Attacks

Defined below are the levels of the security against attacks from third parties (e.g., service providers), including insiders, as seen from the endpoint.

Level 1: This is the level where static, network-based perimeter security controls are in place. At this level, it assumes that there are no security threats within local networks. In other words, the communication is protected only between the GWs, and is vulnerable to attacks from local networks.

NOTE - If the system’s security relies on functions outside of the endpoints, the system’s security level should be recognized as Level 1 or Level 2.

Level 2: If the system’s security relies only on a small number of localized nodes, it is recognized that the system’s security level as level 2. PKI is a good example of level 2 which needs a trusted 3rd party. This level corresponds to NIST zero-trust security.

Level 3: This is the highest level of protection of information. In this level, the users can establish secure end-to-end communication, or store data for with no fear of 3rd parties' attacks.

4. Technology Gaps

This section describes the sufficiency of existing technologies for the security requirements for IOWN, focusing on the following:

- Considering the threats from malicious insiders and dependence on third parties (Security against third party attacks);
- Achieve post-quantum security (Security against computational attacks);

4.1. Authentication and Authorization

An authentication function should establish identifiers and verify the claimed identities and any other entities if these are connected to the IOWN architecture from outside such as users and other networks.

The security measures should support the following functions:

User authentication: establishes the proof of the identity of the functional elements who are connected to the IOWN;

Entity authentication: establishes the proof of the identity of the functional elements in the IOWN during their communications;

Data origin authentication: establishes the proof of identity responsible for the origin of a specific data unit.

Authentication functions play an essential role in protecting confidentiality of the data by ensuring that only authorized parties can access to the data, and in ensuring integrity and authenticity of data.

User authentication has already been the subject of much discussion, and it is recommended that the user authentication function in IOWN, for example, be handled in accordance with the following document. [NIST SP 800-63B] [NIST Multi-Factor Authentication]

This document focuses specifically on entity authentication. (data origin authentication can be accomplished with the same techniques as entity authentication)

An authentication function should employ entity authentication between relevant functional elements before communicating data.

Existing Technologies for Authentication

TODAY's mainstream: Digital Signature Algorithms DSA, ECDSA, EdDSA and RSA

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. (excepts from the abstract of the following document) [NIST FIPS 186-4]

DSA, ECDSA, EdDSA, and RSA are based on mathematical problems that are difficult to solve. These algorithms are recommended by NIST and have established safety in existing threats. They can be used without special equipment. Therefore, it is easy to install in a variety of information systems and can be used for large-scale NWs. Security is maintained by making the key length sufficiently long. Processing speed is slower than the common key method. If a third party such as a CA (Certificate Authority) is involved when verifying digital signatures, there is a risk of leakage.

Some new quantum computer algorithms will soon solve some of the above mathematical problems in real time. So, some of the digital signature cryptography-based digital signature methods are no longer secure in a quantum computing era.

The signature algorithms for authentication that NIST currently recommends for use and their key lengths can be found in [NIST SP 800-131A Rev. 2].

PQC based method

PQC (Post-quantum cryptography) uses cryptographic algorithms based on mathematical problems that are difficult to solve by a quantum computer. It can be used for key exchange and digital signature. There are several approaches: Lattice-based cryptography, Multivariate cryptography, Hash-based cryptography, Code-based cryptography, etc. These are believed to be enough hard problems even for quantum computers to solve.

PQC can be used without special equipment. Therefore, it is easy to install in a variety of information systems. However, some algorithms may have to be improved as computers and their capabilities evolve. If a third party, such as a CA (Certificate Authority,) is involved when verifying digital signatures, there is a risk of leakage. In addition, PQC has very limited track record of being used in commercial systems, and its security against existing threats has not yet been established. Therefore, hybrids with modern cryptography are being discussed.

The selected digital signature algorithm of NIST's PQC standardization can be found here. [NIST PQC Selected Algorithms 2022]

PSK-based methods

Authentication using a pre-shared symmetric key. A pre-shared key is a secret key that has been established between the parties who are authorized to use it by means of some secure method (e.g., using a secure manual-distribution process or automated key-establishment scheme) [NIST SP 800-133 Rev. 2]. Set a common key for multiple devices and check for a match when authenticating. If the mechanism requires the same key to be used and set all over again, it is not suitable for large-scale NWs. If a third party intervenes to share the key, there is a risk of leakage.

Existing Technologies for Authorization

To maintain confidentiality by granting access to resources only to authorized entities, authorization is also an important factor along with authentication. According to the Zero Trust approach [NIST SP 800-207], authentication and authorization should be operated in an integrated manner, taking the following three points into consideration.

- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by dynamic policy
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed

However, at present, there are no notable changes in authorization requirements in the context of E2E data protection and post-quantum security, and each actual system should be considered separately based on the Zero trust approach.

4.2. Data Encryption

Existing Technologies for Key Exchange

Today’s mainstream methods

Existing public key cryptography–based key exchange methods including Diffie-Hellman and RSA are based on mathematical problems which take a long time to solve with non-quantum computers. An eavesdropper needs to solve difficult mathematical problems to eavesdrop on the keys. When the mathematical problems are difficult to solve for the computers, the existing public key cryptography-based key exchange methods are regarded as secure.

However, if the eavesdroppers have the time combined with the enormous computer resources required to address these problems, the existing public key cryptography–based key exchange methods can be broken. In addition, new computing paradigms using quantum computers have introduced new approaches to eavesdrop the keys. Some new quantum computer algorithms can solve the some of the above mathematical problems in real time. So, the some of existing public key cryptography-based key exchange methods are no longer secure in a quantum computing era.

PQC-based methods

These are key establishment methods that utilize PQC as described in the Authentication section. PQC is just a mathematical algorithm. Therefore, it is easy to install in a variety of information systems. However, some algorithms may have to be improved as computers and their capabilities evolve. PQC has almost no track record of being used in commercial systems, and its security against existing threats has not yet been established. Therefore, hybrids with modern cryptography are being discussed.

The selected key establishment algorithm of NIST's PQC standardization can be found here. [NIST PQC Selected Algorithms 2022]

QKD-based methods

QKD (Quantum Key Distribution) is another approach for the key exchange in a quantum computing era. In QKD, the transmitter and the receivers (QKD modules) connected via optical fibers share the keys which are never eavesdropped based on quantum theory. The transmitter sends a series of single photons which encode encryption key information to the receiver. Quantum theory clarifies that no one can eavesdrop on the photons without the receiver detection. Based on the exchanged photon information without eavesdropping, the transmitter and the receiver create and share encrypted key information which is never eavesdropped [BB84]. Since QKD uses a single photon source and detector hardware, the cost of QKD is higher than the existing key exchange methods. In addition, QKD has a limitation on distance, speed and communication style of key exchange (approximately, 100km distance for the longest, several mega bit per second for the highest, point-to-point style communication for the current technology). This limitation comes from the nature of photons/quantum. However, networking QKD (referred as QKD Network, QKDN) overcomes these limitations and enables to deploy large scale QKD secure key distribution platform. The concept of QKDN can be realized in combination with other security solutions including PQC and trusted node as described in [ITU-T Y.3800].

NOTE- The details of technical limitations of a QKD link (optical fiber link to transmit a photon signal) are described in [ITU-T FG QIT4N D2.4].

Quantum key distribution increases infrastructure costs and insider threat risks. QKD networks frequently necessitate the use of trusted relays, entailing additional costs for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration. Quantum key distribution increases the risk of denial-of-service attacks. The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial-of-service is a significant risk for QKD. [NSA QKD and QC]

Existing Technologies for Encryption

AES [NIST FIPS 197]

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

The AES algorithm is faster than public key cryptography. In addition, hardware equipped with an AES accelerator is available, which enables faster processing with lower power consumption than software processing.

The impact of the advent of quantum computers on symmetric key cryptography must also be considered: with Brute-force attacks backed by Grover's algorithm running on top of a quantum computer, the symmetric key length should be doubled from the current one to make it as difficult to find a key to decrypt data as it is today.

OTP

One-time pad (OTP) is a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted by the receiver using a matching OTP and key.

OTP is recommended to ensure the long-term confidentiality of keys because of their information-theoretic security, but OTP requires a pre-shared key the same size as the data being exchanged. This means that this method simply doubles the network bandwidth consumption.

Due to the problem of the key exchange method, it is used only in limited cases, such as when extremely high confidentiality is required and QKD. Because OTP is a stream cipher, encryption and decryption are faster than with block ciphers.

The generation of random numbers (or bits) used for OTP is an important security issue. The security of cryptographic systems that use random bits depends on the entropy of these random bits. Random bit sequences used for OTP can be generated using physical techniques. Quantum mechanics allows the generation of unpredictable random bit sequences because of their probabilistic nature. For this reason, it is desirable to use a random number generated by a non-deterministic random bit generator (NRBG) using quantum mechanics as the random number used for OTP in order to ensure long-term confidentiality of encrypted data.

5. Direction for IOWNsec

Regarding data protection, some existing technologies are expected to become compromised by the advent of quantum computers. Therefore, it is desirable to offer a choice of quantum-safe technologies that can protect data end-to-end in IOWN-based architectures. However, the technologies described in the previous section have their own advantages and disadvantages, and their use alone may not necessarily satisfy the security requirements of future information systems. For example, they do not have much of a track record, so they may suddenly be compromised. They may also require special equipment and thus be applicable to only a limited set of information systems, or they may become vulnerable to third-party threats.

Based on the gap analysis in the previous section and the security requirements of information assets (see section 3), useful security solutions can be selected. But, no single security solution is probably applicable in all cases, especially under the requirements of extremely highly secured information. To truly secure future information systems, additional strategies will be required.

5.1. Multi-Factor Security

5.1.1. 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 as illustrated in the table C-1. (See Appendix C)

5.1.2. Multi-Factor Security for IOWNsec

As for end-to-end data protection, applying the concept of MFS, combining various methods of authentication, key-exchange, encryption/decryption etc. could achieve the required security level which is written at the top of this section, e.g., to counter quantum computers and insiders' threats.

For example, in the case of key exchange, even advanced technologies which are considered for the security issues caused by emergence of quantum computers may not remove the security threats by using a single security technology.

In the key exchange method involving third party service providers from an endpoint's point of view (We call this type of methods Type A), we must consider the threats which are derived from them. It is meaningful that Type A key exchange method is combined with key exchange method which only needs sender and receiver as endpoints (We call this type of methods Type B).

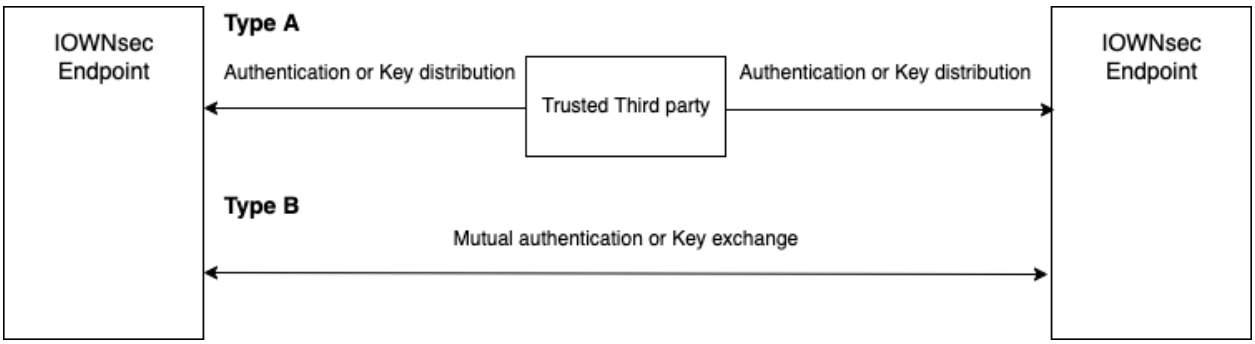

Figure 5.1-1: Difference between Type A and Type B

There are information theoretical security and computational security of key exchange. Key exchange method with information theoretical security is needed for data protection of communications with especially high-level security.

Assuming actual existing technologies and its general implementation examples, QKD which guarantees information theoretical security for key exchange, requires special devices and network infrastructure. Therefore, it is generally considered that QKD is provided by third party as a service provider. Thus, QKD can be seen as an example of Type A. Key establishment means using secure manual distribution (i.e., PSK) is another Type A method with information-theoretic security.

On the other hand, PQC-based technologies, key exchange methods which guarantee computational security, cannot guarantee the ultimate security. However, it can realize key exchange methods between two properly authenticated parities without a third party. Thus, PQC-based key exchange methods can be seen as an example of Type B.

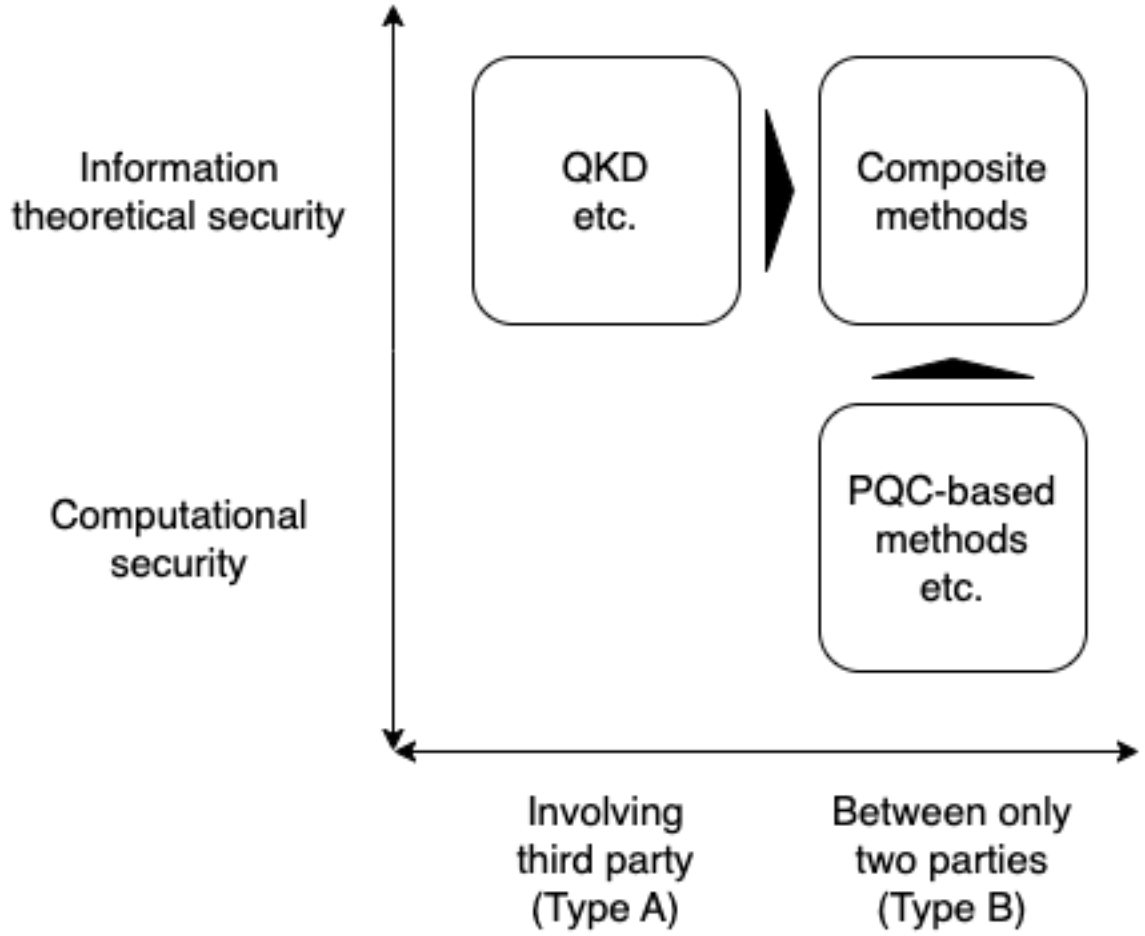

Figure 5.1-2: Image of effect of combining Type A and Type B

Composite methods in Fig.5.1-2 show the combination of key exchange methods Type A (e.g., QKD) and Type B (e.g., PQC-based technologies) by MFS. Even if the Type A methods (e.g., QKD) have information-theoretic security in the protocol, there is still a risk of a trusted third party (TTP). On the other hand, Type B methods (e.g., PQC-based key exchange) are computational security in terms of cryptographic strength but can eliminate the risk of TTPs as much as possible. Therefore, by using a combination of Type A and Type B methods, it is possible to have both information-theoretic security against quantum computers and resistance against TTP.

Assuming that the advantage of both is preserved in MFS, the effectiveness of combining Type A and Type B can be understood as shown in figure 5.1-3, using a concrete example. QKD, an example of a Type A method, is an information-theoretically secure protocol, but there is a Trusted Third Party (TTP) risk when using a third-party service such as the QKD network that performs key relay. In addition, since QKD generally requires dedicated equipment, a separate data protection method between the endpoint and the dedicated equipment must be provided, increasing the risk of internal attacks. On the other hand, the key exchange method using PQC, an example of a Type B scheme, is computationally secure in terms of cryptographic strength, but the risk of TTP can be eliminated as much as possible because key exchange is possible only between endpoints. It can also be implemented directly in software on endpoints, minimizing the risk of internal attacks. Therefore, by using QKD and PQC-based key exchange methods together, it is possible to provide both information-theoretic security for quantum computers and resistance to internal attacks and TTP.

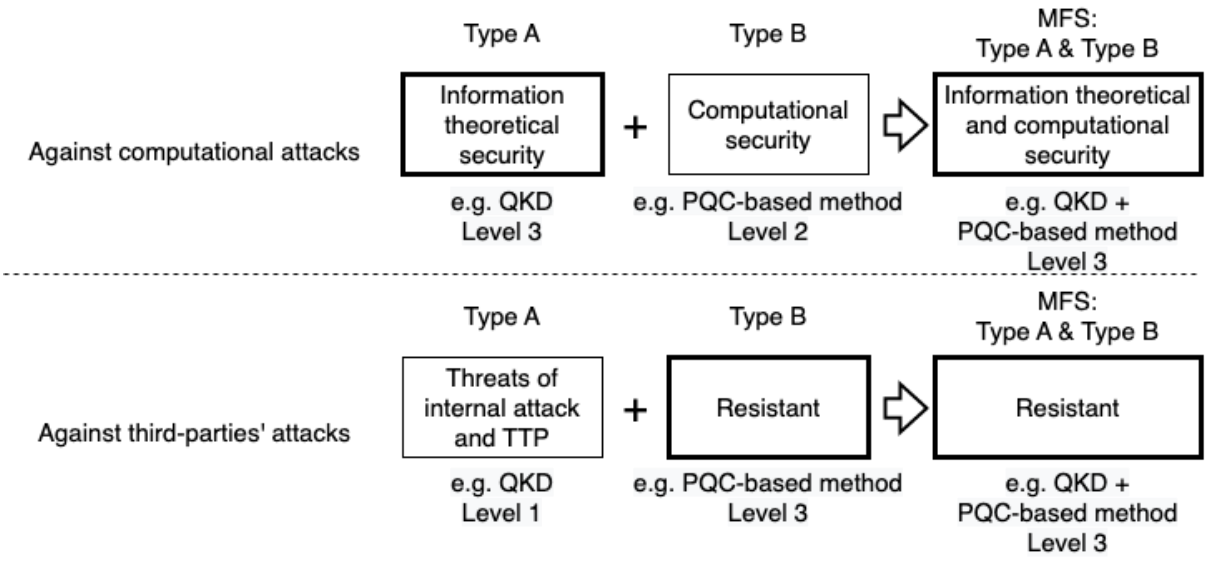

Figure 5.1-3: Image 1 of enhanced attack resistance through combination of technologies

As another MFS option is combining cryptographic algorithms of different characteristics, or being able to switch them quickly. This can help prepare against future algorithm compromise. At present, there are several post-quantum cryptographic algorithms that have been proposed, including lattice-based cryptographic algorithms, code-based cryptographic algorithms, multivariate cryptographic algorithms, hash-based signatures, and others. However, for most of these proposals, further research is needed to gain more confidence in their effectiveness. [NIST PQC Standardization Call for Proposals] New cryptographic algorithms are at high risk of being compromised by a sudden discovery of new attack methods. Since it is quite possible for a cryptographic technique to be suddenly compromised, a combination of multiple post-quantum cryptographic algorithms can be used to prepare for a cryptographic algorithm compromise.

The effectiveness of combining multiple post-quantum cryptographic algorithms (Type B) can be understood as shown in figure 5.1-4. The goal of a combination of multiple post-quantum cryptographic algorithms is to ensure that the desired security property holds if one of the component schemes remains unbroken [Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH].

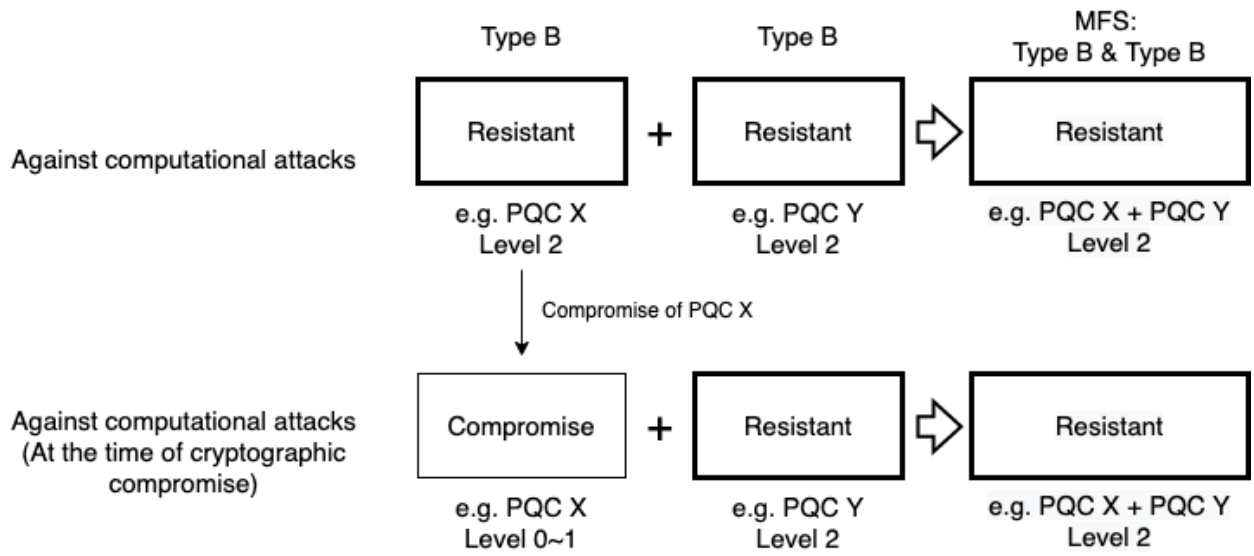

Figure 5.1-4: Image 2 of enhanced attack resistance through combination of technologies

A specific example of MFS is shown in the figure 5.1-5, where Type A and Type B key exchange methods are combined. The keys for data encryption are generated by combining the two keys obtained in both methods.

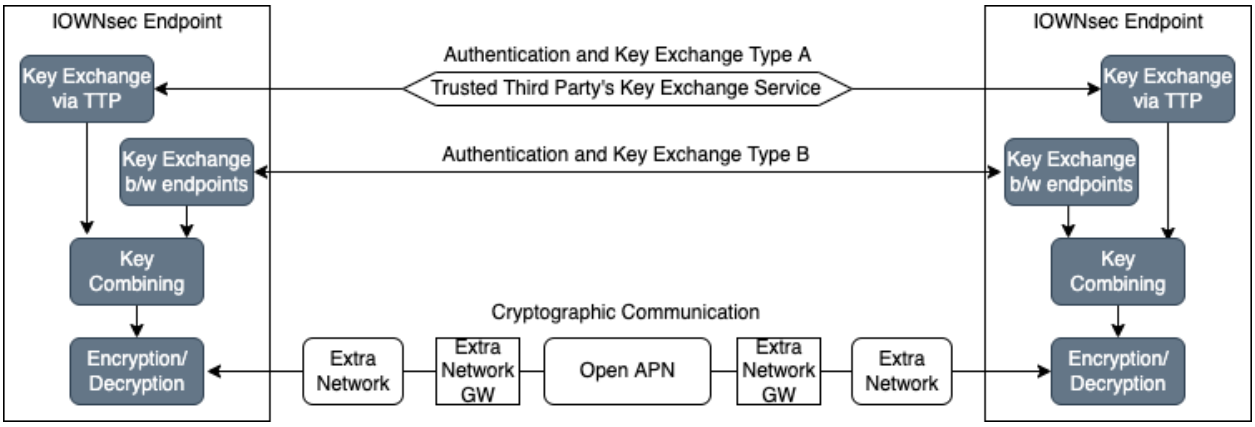

Figure 5.1-5: Specific example of multi-factor security

6. High Level Architecture and Examples

6.1. Functional Architecture/Component

6.1.1. IOWNsec Static Meta Functional Architecture/Components

This section describes the functional architecture/components which enables a functioning MFS architecture.

The functional components of MFS can be divided into two major categories. One is a set of components to be provided by entities including endpoints.

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.

The other is a set of components to be provided on the network side.

This group of components includes security methods provided by third parties and network management functions to control MFS.

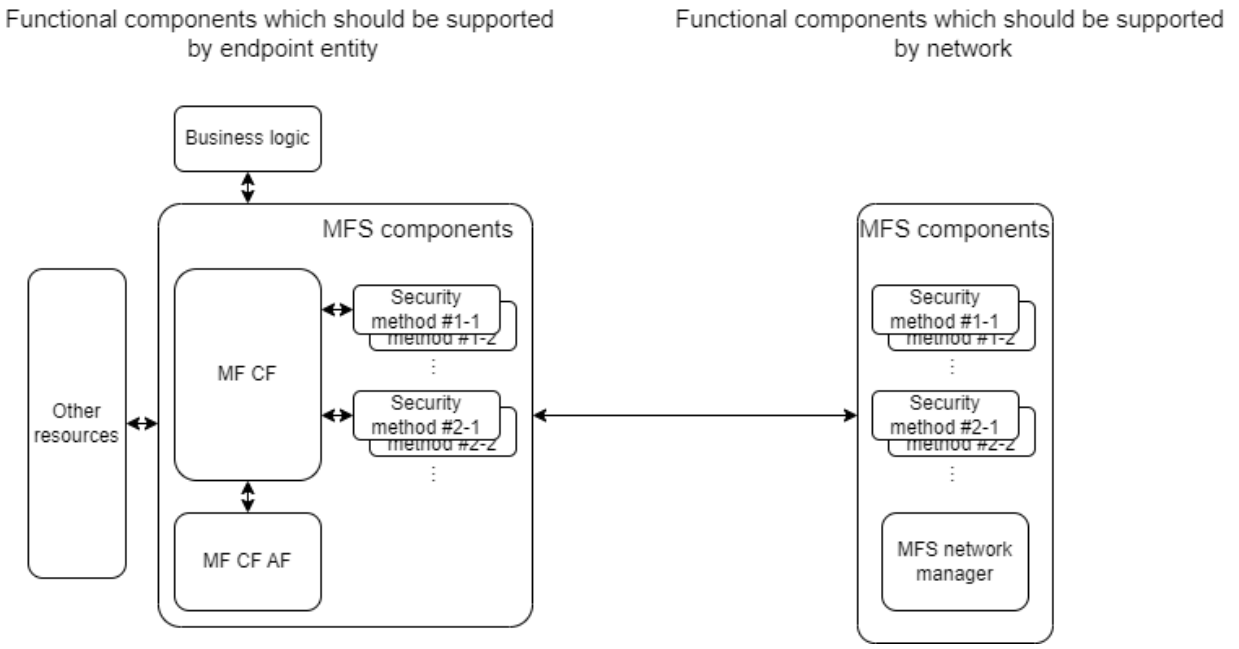

Figure 6.1-1: IOWNsec static meta functional architecture

Business logic: Business logic is the main feature that characterizes an application and is usually implemented in the application process. The MFS components are called from the business logic.

MF CF (control function): MF CF controls the utilization of a single or a combination of Security methods as needed for the security level required/requested/needed by the Business logic.

MF CF AF (adaptive function): To leverage security level of each Security method, MF CF AF adaptively add additional process for Security method's results, e.g., Key combination.

Security method: A security methods for data protection, e.g., authentication method, key exchange method.

Other resources: Resources in end node which are utilized by MFS components, e.g., key store.

MFS network manager (optional): MFS network management is responsible for controlling and managing the MFS components across multiple locations.

6.1.2. Example of IOWNsec Static Functional Architecture/Components

This is an example of MFS. In this case, multiple authentication methods and multiple key exchange methods are used to strengthen the data protection.

Multiple authentication methods are used in a combined way to secure the authentication because each authentication method will supplement other methods' vulnerabilities. When these authentication methods use different authentication factors, it is called MFA.

On the other hand, the use of multiple key exchange methods could realize information-theoretic security and security for any external/internal parties' threats. For example, QKD and key exchange method which does not require any third-party, are used at a same time, QKD realizes information-theoretic security and the other key exchange method avoids the risk of any third-parties compromising security.

In the case of key exchange, it is necessary to combine the keys for cryptographic application, then key combiner is needed as MF CF AF.

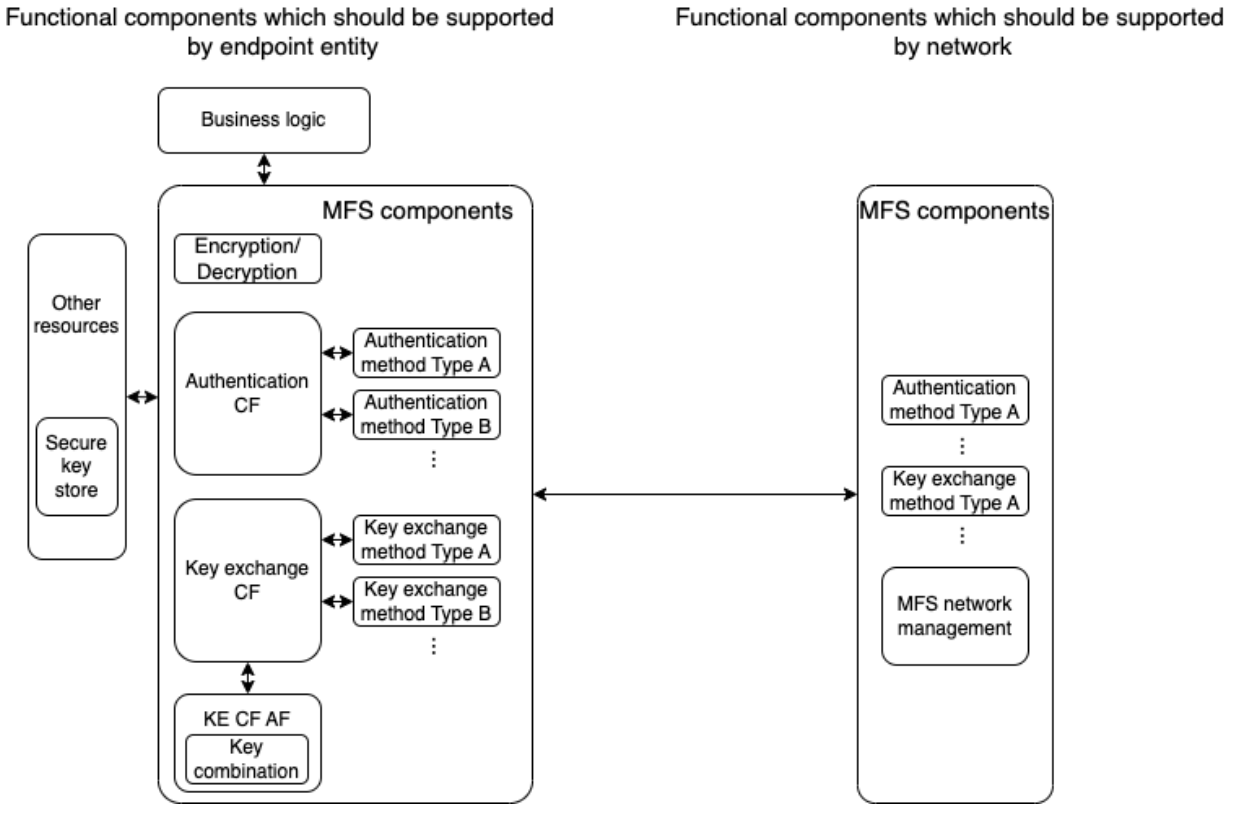

Figure 6.1-2: Example of IOWNsec static functional architecture

Authentication CF: Authentication CF utilizes one or more authentication methods individually or multiply.

Key exchange CF: Key exchange CF utilizes one or more key exchange methods individually or multiply.

KE (Key exchange) CF AF: KE CF AF combines keys of each Key exchange methods to create encryption key.

6.2. Interface between Functional Components/Dynamic

6.2.1. IOWNsec Dynamic Meta Functional Architecture Example 1

MF CF realizes that the required security level utilizing one or more Data protection methods. By the request of Business logic, MF CF performs the security function/data protect function, then returns the result of the requested security function/data protect function to the business logic.

In this example, MF CF performs multiple means of authentication.

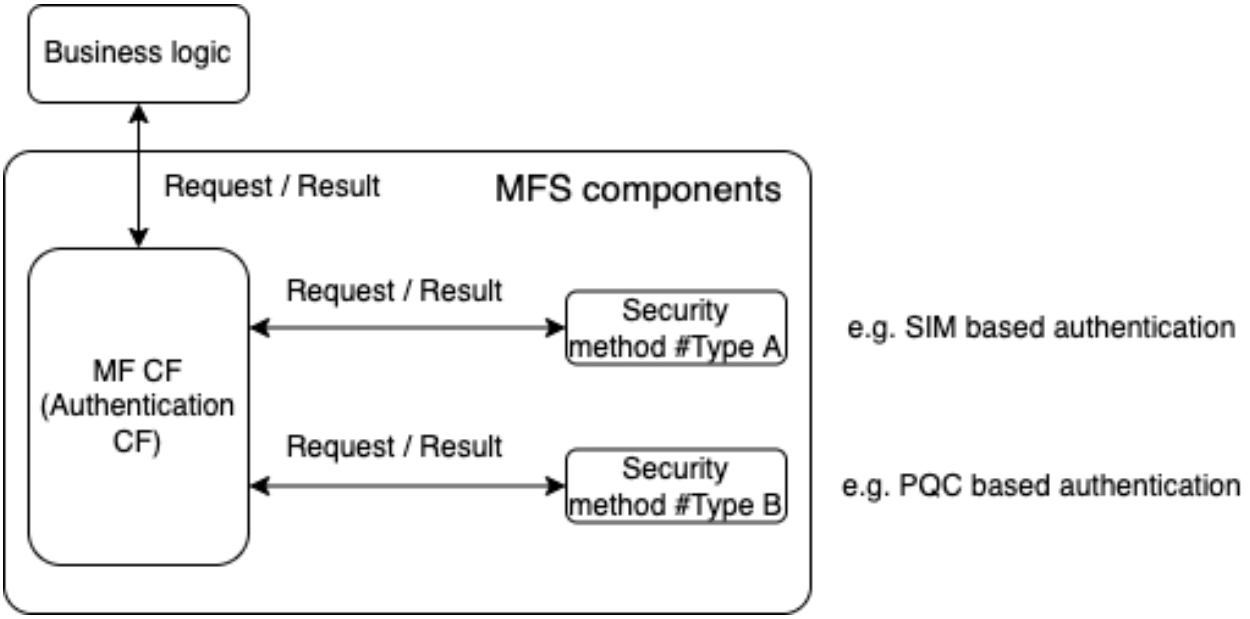

Figure 6.2-1: Example of operation to realize MFA

6.2.2. IOWNsec Dynamic Meta Functional Architecture Example 2

By the request of Business logic, MF CF also coordinates MF CF AF and other resources to add the security function/data protect function to the original ones, then returns the result of the requested security function/data protect function.

In this example, the MFCF executes multiple key exchange means, the resulting two keys are combined in the MF CF AF, and the combined key is stored in the key store.

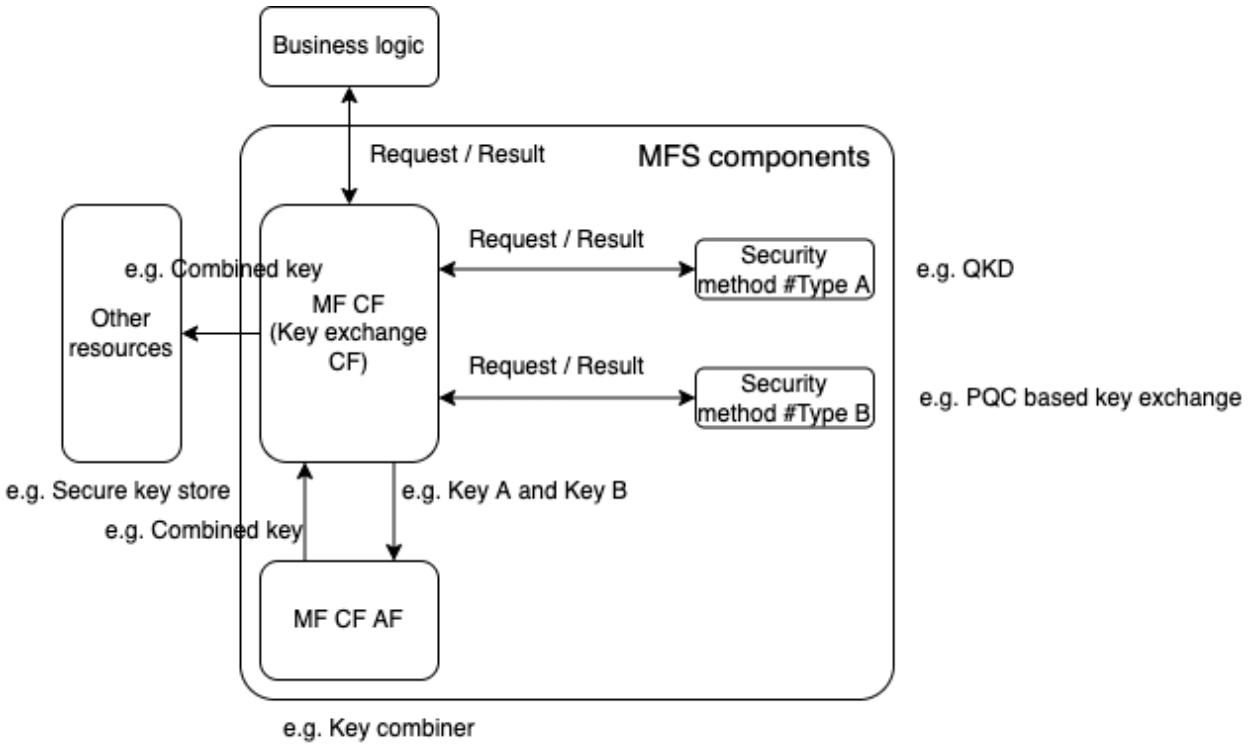

Figure 6.2-2: Example of operation to realize hybrid key exchange

6.3. Mapping: Functional Components to Concrete Entities

6.3.1. Multi-factor Security Network Architecture

As explained in Section 3, high availability is important for achieving high security requirements over the IOWN architecture. To achieve high availability, MFS components require complete life cycle management such as state management, monitoring, and failure management. Moreover, a mechanism to ensure the availability of the MFS components is also needed.

Fig. 6.3-1 shows the MFS network architecture that is mapping to the diagram representing the IOWNsec static meta function architecture in Section 6. The definitions of the logical functions are as follows.

- MFS function node is the managed entity which is the set of functions in an endpoint necessary to provide MFS. It includes the MF CF and MF CF AF functions.
- MFS logical link is the managed entity which is the set of connections between MFS function nodes.
- MFS network is the managed entity which consists of MFS function nodes and MFS logical links.
- MFS network manager (optional) is responsible for the life cycle management of MFS function nodes, MFS logical links, and MFS network. It may communicate with an external network manager to request a network such as out-of-band control channels and key exchanges, and to get a network connectivity status information.

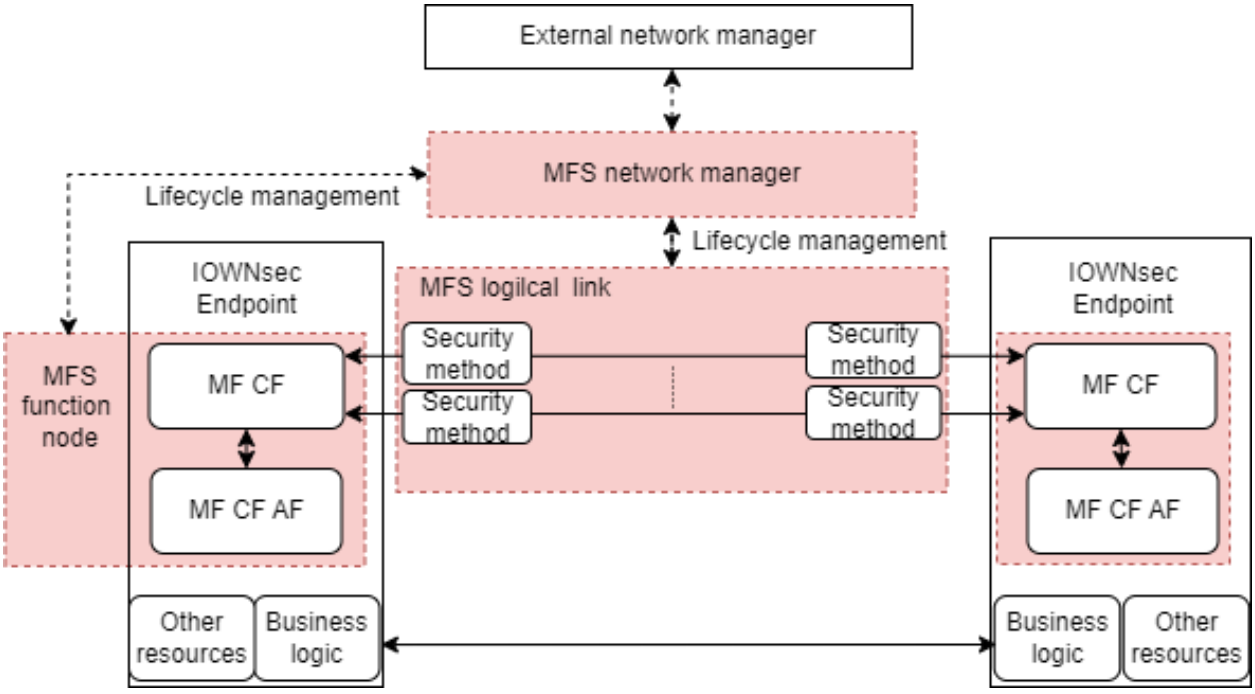

Figure 6.3-1: Multi factor security network architecture

Fig 6.3-2 shows an example of the key exchange. Secure communication is achieved by combining multiple security methods to generate a key and encrypting the communication. It is recommended that MFS function node be independent of cryptographic protocols and hardware implementation. Control channel of MFS logical link is hardware implementation agnostic and control channel between encryption/decryption is hardware implementation dependent.

In addition, if key exchange communication uses the same route as cryptographic communication, there is a risk of eavesdropping together. Thus, separating key exchange and communication paths is important for risk distribution. MFS network management may communicate with external network managers to establish separate out-of-band control channels, key exchanges, and cryptographic communication paths.

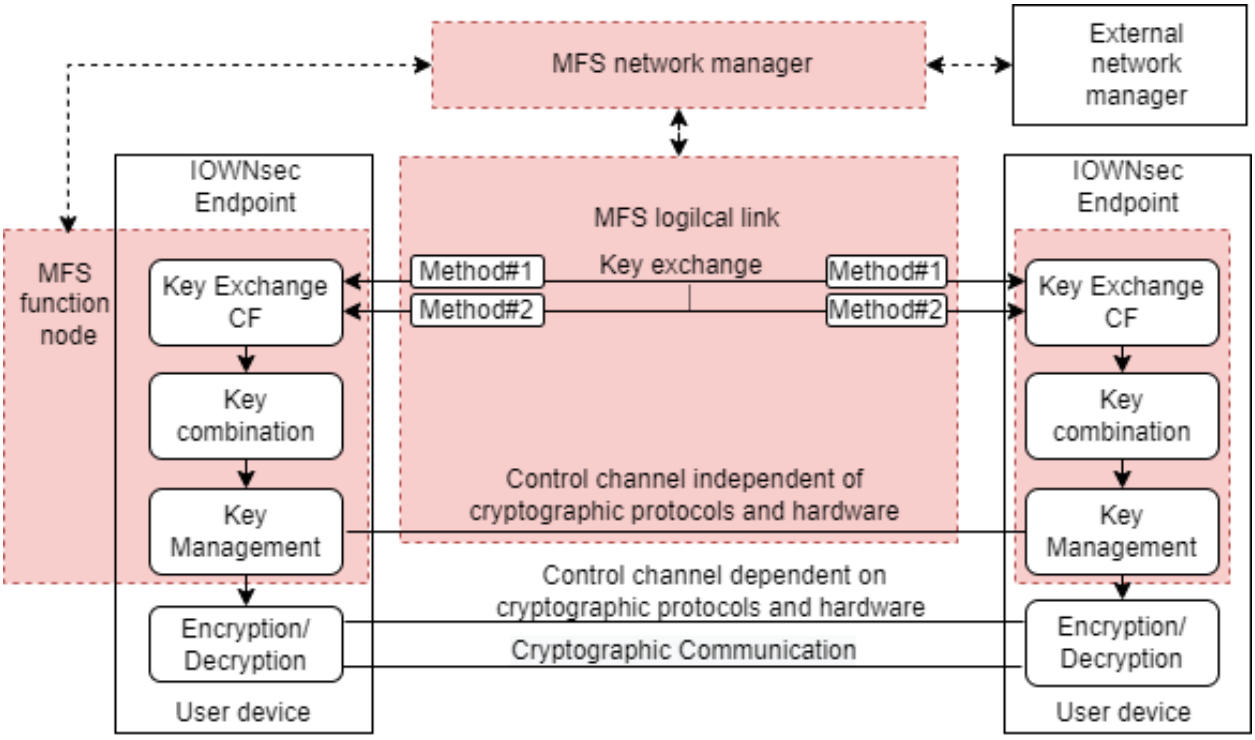

Figure 6.3-2: Example of key exchange

6.3.2. Specific System Architecture Reference Examples for MFS

In this subsection, example physical implementations of MFS are described in the following two use cases.

Use case 1: Communication between customer premise device and server. The communication endpoints are the application processes of a customer premise device and a server.

- Example 1 shows that MFS (PSK-based key exchange and PQC-based key exchange) is implemented on the application processes of a customer premise device and server which is the endpoint.

Use case 2: Communication between servers. The communication endpoints are the application processes of servers.

- Example 1 shows that MFS (PQC-based key exchange and QKD) is implemented on the application process of the server which is the endpoint.

- Example 2 shows MFS (PSK-based key exchange and PQC-based key exchange) is implemented on the Network interface card which is the near-endpoint.

Use case 1 - Example 1: MFS (PSK-based key exchange and PQC-based key exchange) on the endpoint

In the communication pattern between the CPE's smart phone and the server, an example system architecture is shown in Figure 6.3-3 where key exchange is a hybrid of PSK using TTP and PQC between endpoints, and the resulting keys are combined to generate encryption/decryption keys.

- On the smartphone, each component of the MFS is located on the application which is the endpoint, and the subscriber identity module (SIM) is used to store the PSK.

- On the server, each component of the MFS is located on the application process which is the endpoint, and the hardware security module (HSM) is used to store the PSK.

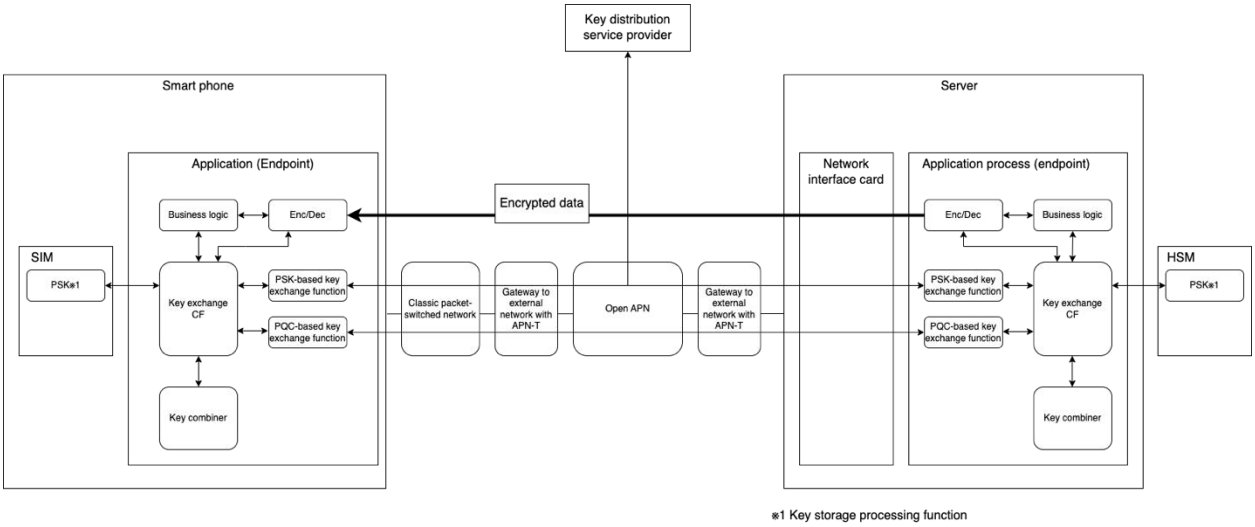

Figure 6.3-3: Specific example of MFS system architecture for key exchange using PSK (Type A) and PQC (Type B) on endpoint

Use case 2 - Example 1: MFS (External QKD and PQC-based key exchange) on the endpoint

In the communication pattern between the servers, an example system architecture is shown in Fig.6.3-4. In this case, QKD, PQC, or both of them is utilized for key exchange. The resulting keys are used at outer and inner encryption/decryption functions.

- On the server, each component of the MFS except for the QKD node, which requires dedicated hardware, is located on the application process which is the endpoint. In this implementation example, Data protection between the endpoint and the QKD node should be considered separately. (see Appendix D) For example, it is also possible to protect the link between the endpoint and the QKD node using PQC or PSK-based pairing.

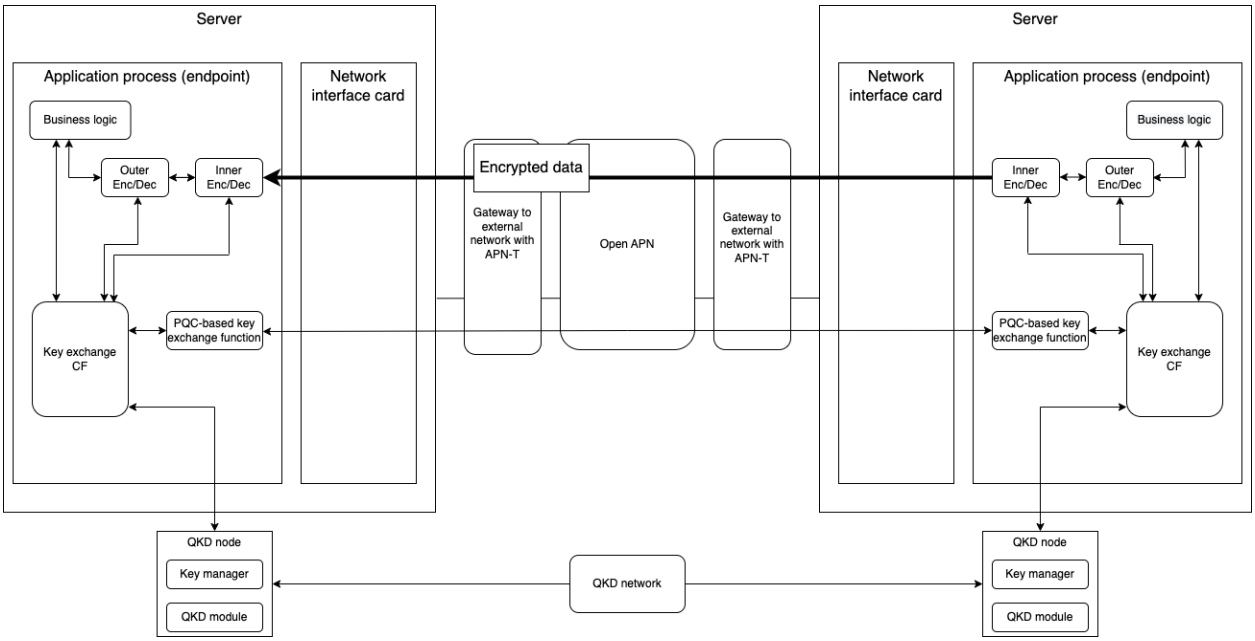

Figure 6.3-4: Specific example of MFS system architecture for key exchange using QKD (Type A) and PQC (Type B) on endpoint

Use case 2 - Example 2: MFS (PSK-based key exchange and PQC-based key exchange) on the near-endpoint

In the communication pattern between the servers, an example system architecture is shown in Figure 6.3-5 where key exchange is a hybrid of PSK using TTP (Type A) and PQC between endpoints (Type B), and the resulting keys are combined to generate encryption/decryption keys.

- On the server, each component of the MFS is located in trusted execution environment (TEE) on the Network interface card (e.g., DPU/IPU/Smart NIC) which is the near-endpoint, and the HSM is used to store the PSK. Although described as an example of using TEE and HSM to protect the Network Interface Card execution environment and the key, measures for protecting against malicious acts on Network interface card as the near-endpoint is outside of the scope of this document. In other words, the actual security level of this system depends on implementation. Data protection between the endpoint and the Network interface card should also be considered separately.

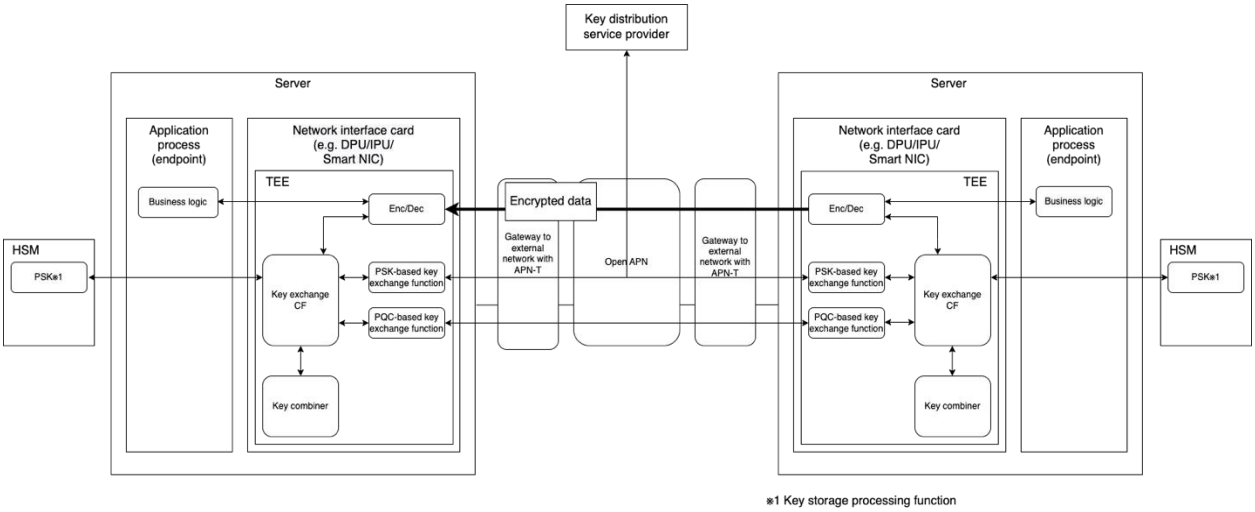

Figure 6.3-5: Specific example of MFS system architecture for key exchange using PSK (Type A) and PQC (Type B) on near-endpoint

7. Conclusion

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 architecture 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 with a single solution. It is realistic way to introduce MFS that combines multiple security measures. This reference document describes the MFS architecture that IOWN architecture 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.

References

[BB84]: C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984,

[IOWN GF ST Outlook]: IOWN Global Forum, “System and Technology Outlook,” 2021, https://iowngf.org/technology/

[IOWN GF AIC UC]: IOWN Global Forum, “AI-Integrated Communications Use Case Interim Report, Version 2.0,” 2021, https://iowngf.org/use-cases/

[IOWN GF CPS UC]: IOWN Global Forum, “Cyber-Physical System Use Case Interim Report, Version 2.0,” 2021, https://iowngf.org/use-cases/

[IOWN GF CPS RIM]: IOWN Global Forum, “Reference Implementation Model (RIM) for the Area Management Security Use Case,” 2022, https://iowngf.org/technology/

[IOWN GF Open APN FA]: IOWN Global Forum, “Open All Photonic Network Functional Architecture,” 2021.https://iowngf.org/technology/

[IOWN GF DCI]: IOWN Global Forum, “Data-Centric Infrastructure Functional Architecture”, 2022, https://iowngf.org/technology/

[IOWN GF IDH]: IOWN Global Forum, “Data Hub Functional Architecture,” 2022, https://iowngf.org/technology/

[ITU-T FG QIT4N D2.4]: ITU-T Technical Report, Quantum key distribution network transport technologies (24 November 2021), https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-QIT4N-2021-D2.4-PDF-E.pdf

[ITU-T Y.3500]: ITU-T Recommendation Y.3500, Information technology - Cloud computing - Overview and vocabulary (2014,8), https://www.itu.int/rec/T-REC-Y.3500-201408-I

[ITU-T Y.3800]: ITU-T Recommendation Y.3800, Overview on networks supporting quantum key distribution (2019,10), https://www.itu.int/rec/T-REC-Y.3800/en

[MITRE AT&CK] https://attack.mitre.org/

[NIST FIPS 186-4] National Institute of Standards and Technology (NIST), FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, https://csrc.nist.gov/publications/detail/fips/186/4/final

[NIST FIPS 197] National Institute of Standards and Technology (NIST), FIPS 197, Advanced Encryption Standard (AES), November 2001, https://csrc.nist.gov/publications/detail/fips/197/final

[NIST Multi-Factor Authentication] National Institute of Standards and Technology (NIST), Multi-Factor Authentication, https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

[NIST PQC Selected Algorithms 2022] National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Selected Algorithms 2022, https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[NIST PQC Standardization Call for Proposals] National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standardization Call for Proposals, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals

[NIST SP800-12 Rev.1]: National Institute of Standards and Technology (NIST), NIST Special Publication 800-12 Revision 1, An Introduction to Information Security (2017,6), (2017,6), https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final

[NIST SP 800-63B] National Institute of Standards and Technology (NIST), NIST Special Publication 800-63B, Digital Identity Guidelines, June 2017, https://csrc.nist.gov/publications/detail/sp/800-63b/final

[NIST SP 800-131A Rev. 2]: National Institute of Standards and Technology (NIST), NIST Special Publication 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths

https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

[NIST SP 800-133 Rev. 2] National Institute of Standards and Technology (NIST), NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, June 2020, https://csrc.nist.gov/publications/detail/sp/800-133/rev-2/final

[NIST SP 800-207] National Institute of Standards and Technology (NIST), NIST Special Publication 800-207, Zero Trust Architecture, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

[NSA QKD and QC] National Security Agency/Central Security Service (NSA/CSS), Quantum Key Distribution (QKD) and Quantum Cryptography (QC), https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH] Eric Crockett, Christian Paquin, and Douglas Stebila, Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH, July 2019, https://eprint.iacr.org/2019/858.pdf

[STRIDE] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[The three types of MFA] skillsoft global knowledge, THE THREE TYPES OF MULTI-FACTOR AUTHENTICATION(MFA), June 2018, https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/

Definitions and Abbreviations

Definitions

For the purposes of this Reference Document, the following definitions apply:

Endpoint: the points where protected data are generated, processed or consumed.

This reference document uses the following terms defined elsewhere:

FDN [IOWN GF ST Outlook]: A Function-Dedicated Network (FDN) function is a network built on top of the Open APN to provide dedicated connection among endpoints to support various traffic and QoS requirements.

Information [NIST SP800-12]: (1) Facts or ideas, which can be represented (encoded) as various forms of data; (2) Knowledge (e.g., data, instructions) in any medium or form that can be communicated between system entities.

Information Security [Y.3500]: Preservation of confidentiality, integrity and availability of information.

Information Security [NIST SP800-12]: Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.

Abbreviations and Acronyms

For the purposes of this Reference Document, the following abbreviations and acronyms apply:

2FA: Two-Factor Authentication

AES: Advanced Encryption Standard

AF: Adaptive Function

AI: Artificial Intelligence

APN: All-Photonic Network

ARP: Address Resolution Protocol

CF: Control Function

CPS: Cyber Physical Space

DCI: Data Centric Infrastructure

DNS: Domain Name System

DoS: Denial of service

DP: Data Plane

DRAM: Dynamic Random-Access Memory

DSA: Digital Signature Algorithm

E2E: End-to-End

ECDH: Elliptic curve Diffie–Hellman key exchange

ECDSA: Elliptic Curve Digital Signature Algorithm

EdDSA: Edwards-curve Digital Signature Algorithm

FDC: Function-Dedicated Computing

FDN: Function-Dedicated Network

FIPS: Federal Information Processing Standards

GPU: Graphics Processing Unit

HSM: Hardware security module

IDH: IOWN Data Hub

IOWNsec: IOWN security

KE: Key Exchange

KM: Key Manager

MFA: Multi-Factor Authentication

MFS: Multi-Factor Security

NIC: Network Interface Card

NIST: National Institute of Standards and Technology

NRBG: Non-Deterministic Random Bit Generator

OSS: Open Source Software

OTP: One Time Pad

PIN: Personal Identification Number

PKI: Public Key Infrastructure

PQC: Post-Quantum Cryptography

PSK: Pre-Shared Key

QKD: Quantum Key Distribution

QKDN: QKD Network

RDMA: Remote Direct Memory Access

RHISM: Reconfigurable High-speed Interconnect and Shared Memory

RIM: Reference Implementation Model

RSA: Rivest-Shamir-Adleman cryptosystem

SIM: Subscriber Identity Module

TEE: Trusted Execution Environment

TLS: Transport Layer Security

USB: Universal Serial Bus

WI: Work Item

Appendix A: Information Assets to be Protected in IOWN GF CPS RIM

The information asset to be protected in CPS use case is data payload of workload. A packet frame layer of Protocol Data Unit (PDU) encapsulating the payload by the network overhead is exchanged over All-photonics network via DCI-GW embedding APN-T(transceiver) for the inter-site network connection. With refereeing to the first edition of the reference implementation model for CPS Area Management security guarding service use case [IOWN GF CPS RIM] illustrating the Figure A-1, the Table A-1 summarizes the information assets element in each segment. [IOWN GF DCI] [IOWN GF IDH]

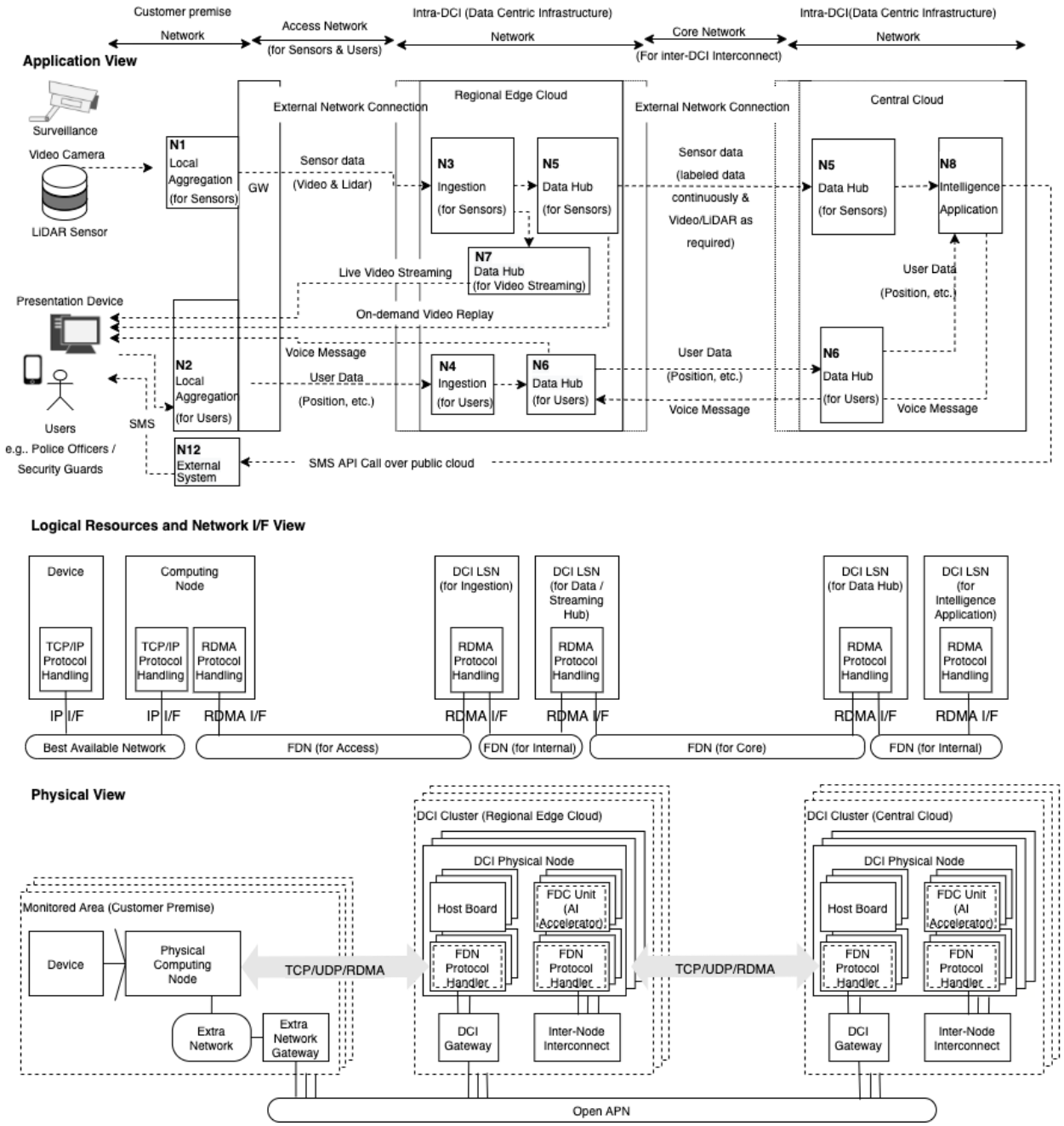

Figure A-1: Overview of application view and network view based on data pipeline diagram

IOWN GF CPS RIM has been described a reference implementation system that surveillance camera video image and LiDAR sensor data with AI to identify criminal activities or accidents for a prompt response and/or action by police and/or security agents. IOWN GF CPS RIM assumes three layers of the vertical distribution of computing sites, that are;

- Customer premises in monitored area such as LiDAR/Surveillance camera or in user site such as Police office
- Regional edge clouds built with IOWN DCI (Data Centric Infrastructure) architecture
- Central clouds built with IOWN DCI (Data Centric Infrastructure) architecture

The following table summarizes a correspondence between elements or links and information assets in IOWN GF CPS RIM.

Table A-1: Relation between elements and information assets in IOWN GF CPS RIM

INFORMATION ASSETS ELEMENTS	FROM	TO	DATA TYPE	STORE TERM
Payload in the link between LiDAR/Surveillance Camera in monitored area via Local Aggregation(N1) and N3(Ingestion of sensor live data in Regional Edge Cloud)	LiDAR in Customer premise/ monitored area	N3(Ingestion Node) in Regional Edge Cloud	LiDAR's Point Cloud data via Local Aggregation (N1) in Monitored area	Temporary in GPU memory or pMEM/DRAM at N3
	Surveillance Camera in Customer premise/ monitored area	N3(Ingestion Node) in Regional Edge Cloud	Surveillance Camera's Video streaming data via Local Aggregation (N1) in Monitored area	Temporary in GPU memory or pMEM/DRAM at N3
Frame layer PDU(FDN) over Bit layer PDU(APN) NOTE1	Local Aggregation N1 in monitored area	DCI in Regional edge cloud	Same as above two columns	Same as above two columns
Payload in link between N7(Data Hub for Live Video Streaming in Regional Edge Cloud) and Presentation device via N2(local Aggregation in Police/Security agent office)	DataHub (N7) in Regional Edge Cloud	Presentation device in Police officer/etc. in Customer premise/police office, etc.	Live Streaming data from DataHub (N7 for video streaming)	Temporary in DRAM/PMEM
Payload in the link between N6 (Data Hub for sensor data in Regional Edge Cloud) and Presentation device via N2(local Aggregation in Police/Security agent office)	DataHub (N5) in Regional Edge Cloud	Presentation device in Customer premise/police office, etc.	On-Demand Video Replay data from Data Hub	Normally store in 1-2 month, but some data store in cold storage/archive based on User's operation policy.
Payload in the link between N6 (Data Hub for sensor data in Regional Edge Cloud) and Presentation device via N2(local Aggregation in Police/Security agent office)	DataHub (N6) in Regional Edge Cloud	Presentation device in Customer premise/police office, etc.	Voice message from Data Hub (N6)	Normally store in 1-2 month, but some data store in cold storage/archive based on User's operation policy.

Payload in the link between N4(Ingestion for user's position data in Regional Edge Cloud) and Presentation device via N2(local Aggregation in Police/Security agent office)	N4(Ingestion Node) in Regional Edge Cloud	Presentation device in Customer premise/police office, etc.	Position data from N2 to N4.	Temporary in DRAM/pMEM
Frame layer PDU(FDN) over Bit layer PDU(APN)	DCI in Regional edge cloud	Local Aggregation N2 in Customer premise	Same as above four columns	Same as above four columns
Payload in the link between Data Hub(N5) in Regional Edge Cloud and Data Hub(N5) in Central Cloud	N5 (Data Hub) in Regional Edge Cloud	N5 (Data Hub) in Central Cloud	Inference result data (labeled data persistently) and Video/LiDAR data as user's required.	Normally store in 1-2 month, but some data store in cold storage/archive based on User's operation policy.
Payload in the link between Data Hub(N6) in Regional Edge Cloud and Data Hub(N6) in Central Cloud via N8 (Intelligence Application)	N6 in Regional Edge Cloud	N6 in Central Cloud	User Data Labeled Object, e.g., JSON with copped image.	Temporary in DRAM/pMEM
Frame layer PDU(FDN) over Bit layer PDU(APN)	DCI in Regional Edge Cloud	DCI in Central Cloud	Same as above two columns	Same as above two columns
Payload in the link between N12(External System) and N8(Intelligence Application) over public Cloud	N8(Intelligence Application) in Central Cloud	SMS of Police officer, etc.	Notification message from Intelligence application (N8 in central Cloud) to Police officers/Security agents via External system(N12) over SMS in public cloud	Temporary in DRAM/pMEM

NOTE1 Local aggregation node (N1) and Ingestion node (N3) have RDMA Interface to share data over memory to AI accelerator engine in Logical Service Node. IOWN DCI TF is starting to explore for RDMA security enhancement in FDN. Cross TF work will be needed in near future.

Appendix B: Positioning of "Threats" in this Version

This version focuses on authentication and encryption as a common data protection security for E2E communication path of the reference model.

Here, this appendix shows the positioning of "threats" in this version as a reference for future study.

Table B-1: Security Threats

SECURITY THREATS		PROTECTION OF INFORMATION	PROTECTION OF INFORMATION SYSTEMS
Network	Spoofing	1st Priority	2nd Priority (TBD)
	Cloning		
	Flooding		
	Sniffing		
Physical	Electromagnetic wave attack, etc.	2nd Priority (TBD)	
Application	Search for application vulnerabilities, and attack from there. End-to-end attacks that target user information and identify specific applications. Link-by-Link attack that targets the lower layer of the application and attacks a wide range of applications. (resource-based threat)		
Human	Money (candy and whip) Unauthorized access using human factors		
Product life cycle	Design: Backdoor creation, etc. in the in-house production process		
	Zero-day attack, etc. (OSS/COTS) in the in-house production process		
	Software: Non-encrypted software code in ROM is easily analyzed by criminals, etc.		
	Development: Maintenance log analysis hack, etc.		
	Manufacturing: Quality test spoofing, etc.		
	Tester: Testing machine with spoofed calibration		

	Logistics: Replacement at Logistics, etc.		
	Operation: Narrowise the monitoring area, etc.		
	Maintenance: Fake software update, etc.		
	Disposal: Fake Disposal -> Spoofing Using Waste, etc.		
Supply Chain	Design: Backdoor creation, etc. by suppliers.		
	Zero-day attack, etc. (OSS/COTS) caused by suppliers		
	Software: Pre-packaged software easily analyzed by criminals, etc.		
	HW materials: compromised information system in factory, etc.		
	Tester: Testing machine from vender with spoofed calibration		
	Service provider: information leakage, etc. due to a wrong configuration and/or a lack of security design.		
Mutual intrusion	In Digital twin: Digital <-> Physical		
	In Social engineering: SNS <-> Human behavior		
	Fake and propaganda: Vision <-> Objection --- connect to “human behavior” or “Common sense”		
Time difference	detection and communication delay make attacking period		
	detection and parching delay make attacking period		
	Report fraud: Reporting fraud (time, scope, intentional denial of charges) may happen. The time lag between reporting fraud and finding facts is a period of attack from the attacker.		
	Judgment gray period: Attack detection is not clear usually and there are gray periods such as forensic periods. This gray period is directly the attack period from the attacker.		

(1) network threats

· Spoofing

Spoofing is when an attacker impersonates an authorized device or user to steal data, spread malware, or bypass access control systems. There are many different types of spoofing, with three of the most common being: IP address spoofing, ARP spoofing, DNS spoofing. It is necessary to recognize threats while being aware of the computing power of post-quantum.

· Cloning

In cyber security, cloning is the process of taking a legitimate document and replacing its normal links with malicious links. This can cause a person who mistakes the document for the original to click on a link that downloads malicious code, such as malware, after mistaking it for a genuine item.

· Flooding

Flooding attack involves the generation of spurious messages to increase traffic on the network for consuming server's or network's resources. Denial of service (DoS) attacks can be flooded with traffic or send information that triggers a crash to the target, so the former method is classified as a Flooding attack.

· Sniffing

Monitoring and intercepting data packets passing through a network with the help of specialized tools called packet sniffers is called “sniffing.” Data packets carry a wealth of information and facilitate the process of incoming and outgoing traffic. There are two types of sniffing- active and passive. As the name suggests, active involves some activity or interaction by the attacker in order to gain information. It is necessary to recognize threats while being aware of the computing power of post-quantum.

(2) Physical threat (electromagnetic wave attack, etc.)

In a physical attack, an attacker gains physical access to a physical asset in the infrastructure system in order to damage it, disable it, steal it, or use it in an undesirable way. In cryptography, electromagnetic attacks are side-channel attacks performed by measuring the electromagnetic radiation emitted from a device and performing signal analysis on it.

(3) Application threat

An application attack consists of cyber criminals gaining access to unauthorized areas. Attackers most commonly start with a look at the application layer, hunting for application vulnerabilities written within code. Though attacks target certain programming languages than others, a wide range of applications representing various languages receive attacks.

· End-to-End: Threats in application processes

Looking at application attacks from the perspective of the communication layer, end-to-end attacks and link-by-link attacks have different target scope of threats. As shown in Fig. B-1, end-to-end attacks focus only on upper application communication without specifying the communication lower layer.

In other words, in an end-to-end attack, the criminal identifies the information that the user must protect, identifies the application, and attacks.

In addition to end-to-end encryption, authentication and authorization are also important because the attack in this case targeting to identify the application or user.

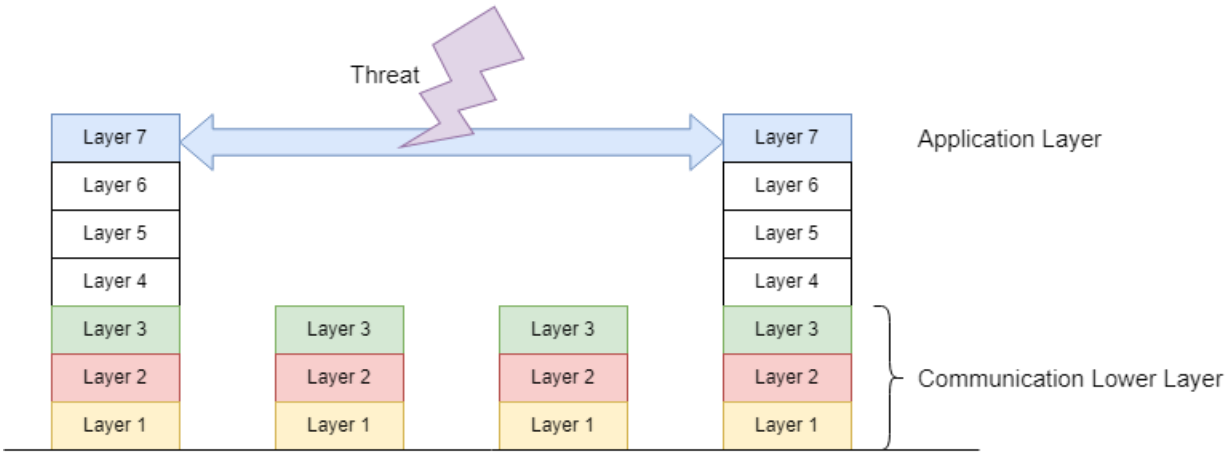

Figure B-1: End-to End Threat in application process

· Link-by-Link: Threats in interface L2 process

As shown in Fig. B-2, Link-by-Link attacks focus specifying the communication lower layer. They do not target specific user or application process.

Attacks that are received without distinguishing applications at layers below the application process, not limited to the L1-L3 interface. It is regarded as an attack that attacks society as a whole without specifying the application or user. The idea of zero trust is emphasized because the target of the attack is not explicit.

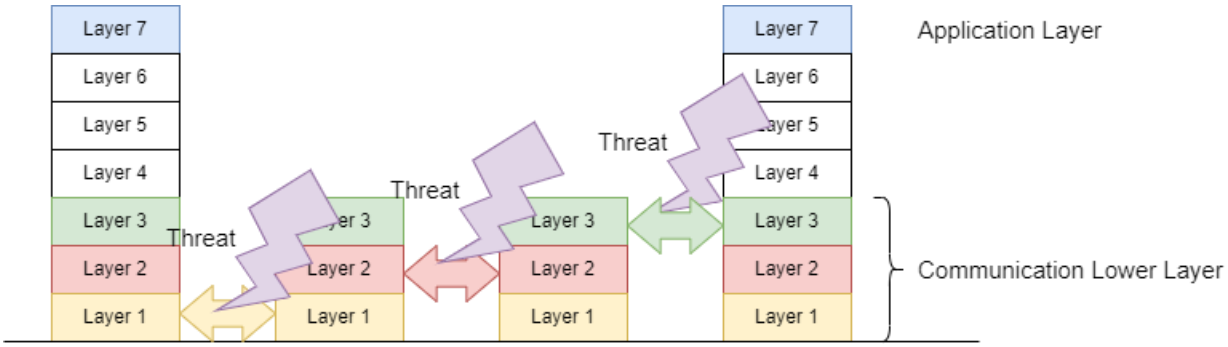

Figure B-2: Link-by-Link Threat in Communication Lower Layers

· Threats in physical layer processes such as Facilities

Criminals physically attack the facility itself. It is used not only as an attack that impairs the business continuity of the facility, but also as an entrance to other attacks. Risk evaluation ask many parameters caused by attack from a different perspective, such as an electromagnetic wave attack or a human-based attack.

(4) Human threat (candy and whip)

Human factors are used by cybercriminals to effect unauthorized access, steal credentials, and infect IT systems and endpoints with malware such as ransomware. The growth of social media, remote working, the use of personal devices, the generation gap, etc. all combine to create new vulnerabilities in an organization's cyber defense. It is necessary to design the monitoring on the assumption that it will be attacked by human-based vulnerabilities.

(5) Product lifecycle threat

It is necessary to capture information security threats within product lifecycle。

· · Backdoor preparation during development --> intrusion during operation

· · Fake Disposal --> Spoofing Intrusion using Disposal Products

· Logistics replacement --> Fire of the capacitor

(6) Threats in supply chain

It is necessary to capture information security threats within supply chain, as can be seen from the case of zero-day vulnerability attacks.

· OSS

· Software materials supplier

· Tester

· Service Provider

· Hardware materials supplier

(7) Threat of mutual intrusion perspective

In the relationship between virtual space and real space in digital twins, or the relationship between social engineering (information space) and human behavior (real space), or the relationships in propaganda which control people's real behavior through artificial false news (information space), in other word, when different world views are interacting, attacks on one worldview can be seen as threats to affect the alternative twin world.

· Intrusion of logical and physical in digital twins

  It refers to the threat of intruding into the real-world system by hacking in the virtual world, so that transactions in the virtual world are indirectly linked to real world currencies.

· Social engineering and human behavior

  Fake information on SNS leads to suicide, or internal information is leaked believing it to be a good thing. It is executed by explicitly targeting specific individuals and should be recognized as a threat.

· Fake news and propaganda

  It's similar to social engineering, but the target is mass, so the impact is bigger. For example, based on fake information, people who receive it all start encrypted communication at a fixed time.

(8) Time difference threat

Moreover, given that cyberattack detection is not timely, it is even necessary to consider information security threats from delay on the supply chain communication.

· Threat of potential bad use period due to detection and communication delay

· Report fraud (time, range, intentional plea)

· Gray judgment period institutional Threat

Appendix C: Multi-factor Authentication (MFA)

In MFA, different types of authentication methods are combined to achieve higher levels of security.

MFA is a method of logon verification where at least two different factors of proof are required. MFA is also referred to as 2FA, which stands for two-factor authentication. MFA helps keep protect your data (email, financial accounts, health records, etc.) or assets by adding an extra layer of security.

There are generally three recognized types of authentication factors:

Type 1 – Something You Know – includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.

Type 2 – Something You Have – includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.).

Type 3 – Something You Are – includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification. [The three types of MFA]

Table C-1: Multi-factor authentication (MFA) as an example of multi-factor security

	NO COPYING & SHARING	NO THEFT	NO FALSE POSITIVE
1: Password	NG	OK (NOTE 1)	OK
2 Hardware Token	OK	NG	OK
3: Biometrics	OK	OK	NG
MFA with 1 and 2	OK	OK	OK
MFA with 1 and 3	OK	OK	OK
MFA with 2 and 3	OK	OK	OK

NOTE 1: We assume that the subject does not store his/her password.

Appendix D: Relationship between QKDN [ITU-T Y.3800] and IOWNsec Model

The relationship between QKDN, an example of a TTP-based key exchange method, and IOWN sec MFS is shown below.

ITU-T Y.3800 defines the functional architecture of QKDN and a user network as shown below.

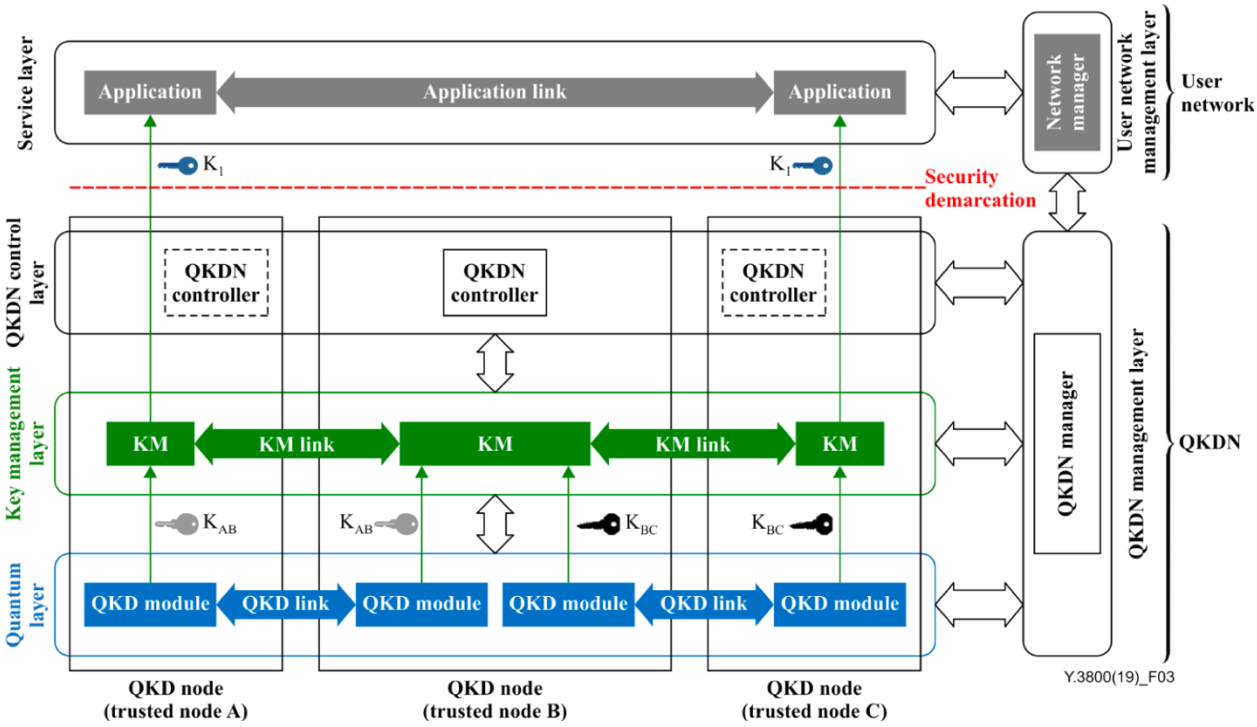

Figure D-1: Illustration of the conceptual structures of a QKDN and a user network [ITU-T Y.3800]

Fig. D-2, which shows a concrete example of MFS, can be rewritten according to the architecture of QKDN as shown below.

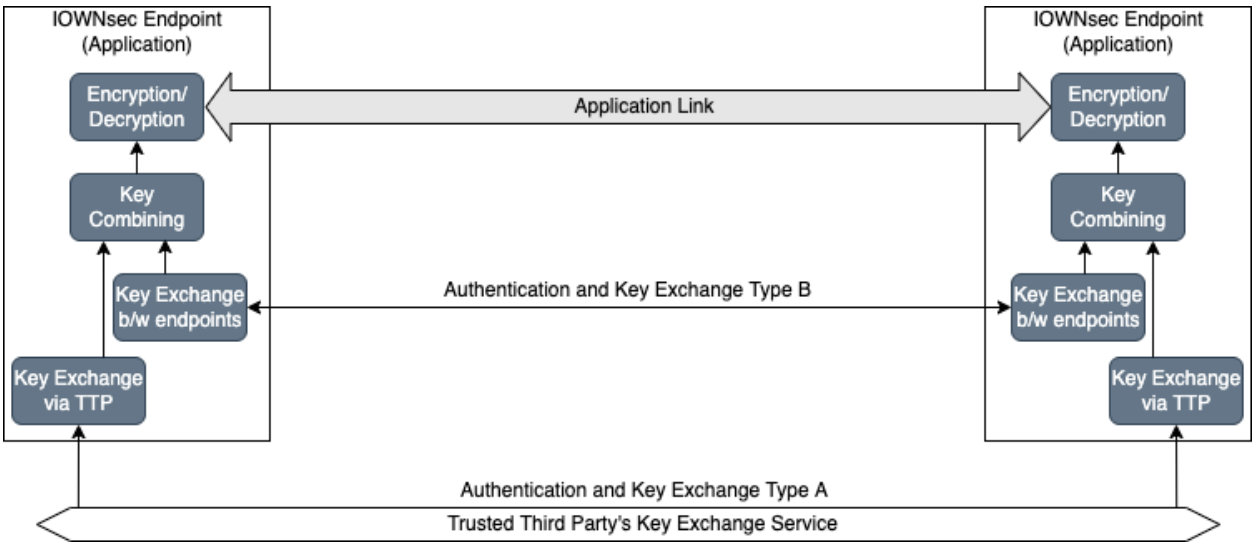

Figure D-2: Specific examples of MFS rewritten to fit the QKDN architecture

The relationship between IOWNsec MFS and the architecture of QKDN is shown in the figure below.

In the QKDN view, IOWNsec should be recognized as an application. In the IOWNsec view, the QKD Infrastructure should be recognized as a trusted third party. IOWNsec MFS receives keys for encryption from outside the security demarcation. For IOWNsec application systems, QKDN can be treated as a method of Type A Key Exchange.

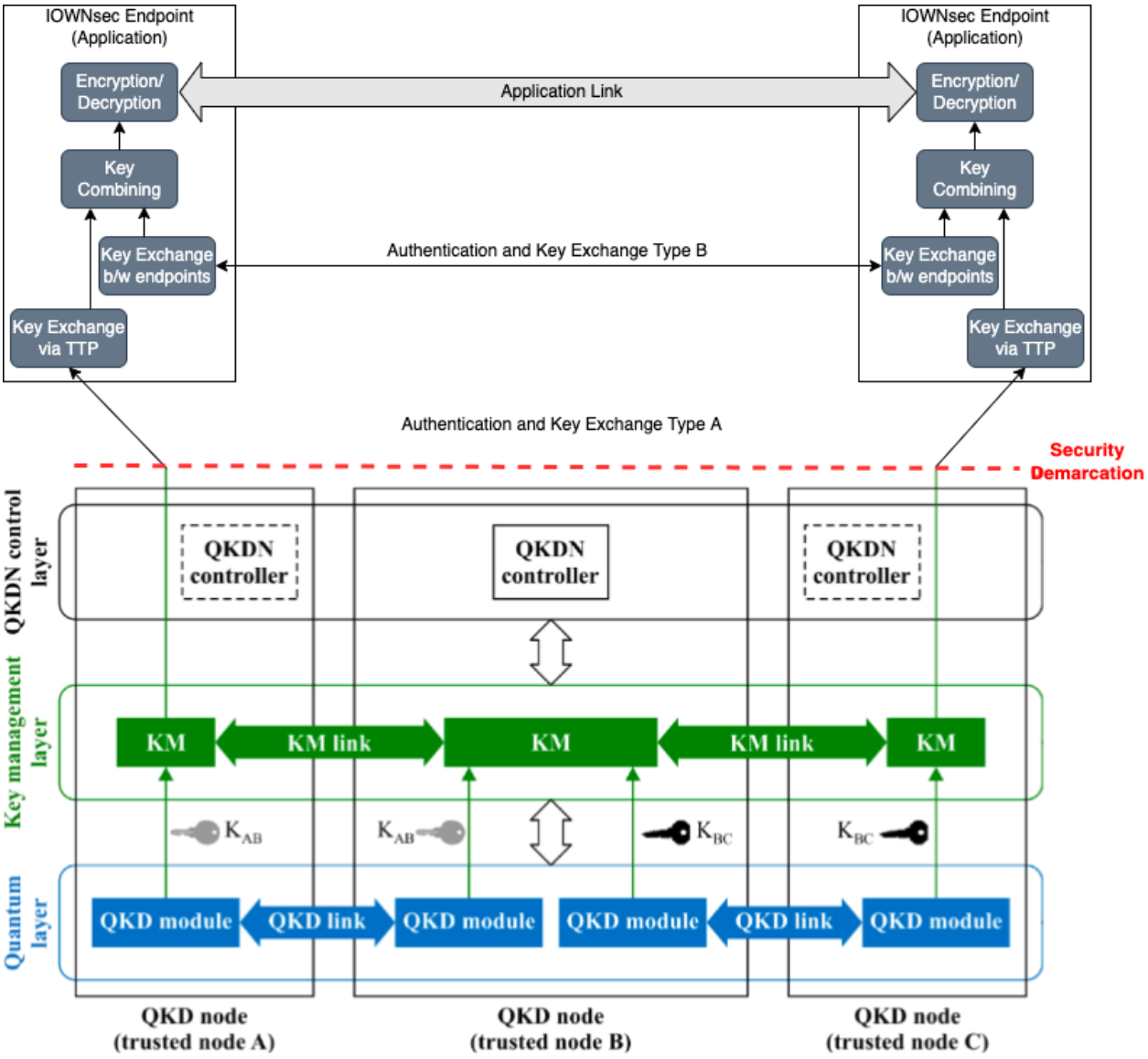

Figure D-3: Relationship between IOWNsec MFS and architecture of QKDN

Appendix E: Key Combining Methods

[NIST SP 800-133 Rev.2] specifies symmetric keys produced by combining (multiple) keys and other data. Note that while the “keys” are required to be secret and established by key exchange schemes which are approved by the NIST, the “other data” need not be kept secret (i.e. keys established by quantum-safe cryptographic algorithms or QKD are “other data” in [NIST SP 800-133 Rev.2]).

These are requirements for key combining.

a) The component symmetric keys shall be generated and/or established independently (and subsequently protected as necessary) using approved methods.

b) Key exchange methods shall support a security strength that is equal to or greater than the targeted security strength of the algorithm or application that will rely on the output key K.

c) Each component key shall be kept secret and shall not be used for any purpose other than the computation of a specific symmetric key K (i.e., a given component key shall not be used to generate more than one key).

[NIST SP 800-133 Rev.2] recommends three methods to generate symmetric keys from the combination of keys and other data.

1. Concatenating two or more keys, i.e., K = K1 || … || Kn.

The length of the generated key equals the sum of the lengths of the keys that have been concatenated. This method does not allow the use of other data.

1. Exclusive-Oring one or more symmetric keys and possibly one or more other items of data, i.e., K = K1 ⊕ … ⊕ Kn ⊕ D1 ⊕ … ⊕ Dm.

The length of each key or other data that is used as input shall be equal to the required length of the resulting symmetric key.

1. A key-extraction process, i.e., K = T(HMAC-hash(salt, K1 || …|| Kn || D1 || …|| Dm), kLen).

The resulting symmetric keys are produced by a hash-based message authentication code (HMAC) function applied on the concatenation of the (multiple) keys and the other data.

…

History

REVISION	RELEASE DATE	SUMMARY OF CHANGES
1.0	February 15, 2023	Initial version