Technology Outlook of Information Security

Classification: APPROVED REFERENCE DOCUMENT

Confidentiality: PUBLIC

Version 2.0

February 05, 2025

[Tech Outlook of InfoSec]

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org

Legal [draft]

THIS DOCUMENT HAS BEEN DESIGNATED BY THE INNOVATIVE OPTICAL AND WIRELESS NETWORK GLOBAL FORUM, INC. (“IOWN GLOBAL FORUM”) AS AN APPROVED REFERENCE DOCUMENT AS SUCH TERM IS USED IN THE IOWN GLOBAL FORUM INTELLECTUAL PROPERTY RIGHTS POLICY (THIS “REFERENCE DOCUMENT”).

THIS REFERENCE DOCUMENT IS PROVIDED ”AS IS” WITH NO WARRANTIES WHATSOEVER, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT OF THIRD PARTY RIGHTS, TITLE, VALIDITY OF RIGHTS IN, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, REFERENCE DOCUMENT, SAMPLE, OR LAW. WITHOUT LIMITATION, IOWN GLOBAL FORUM DISCLAIMS ALL LIABILITY, INCLUDING WITHOUT LIMITATION LIABILITY FOR INFRINGEMENT OF ANY PROPRIETARY RIGHTS AND PRODUCTS LIABILITY, RELATING TO USE OF THE INFORMATION IN THIS REFERENCE DOCUMENT AND TO ANY USE OF THIS REFERENCE DOCUMENT IN CONNECTION WITH THE DEVELOPMENT OF ANY PRODUCT OR SERVICE, AND IOWN GLOBAL FORUM DISCLAIMS ALL LIABILITY FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOST PROFITS, LOSS OF USE, LOSS OF DATA OR ANY INCIDENTAL, CONSEQUENTIAL, DIRECT, INDIRECT, PUNITIVE, EXEMPLARY, OR SPECIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY OR OTHERWISE, ARISING IN ANY WAY OUT OF USE OR RELIANCE UPON THIS REFERENCE DOCUMENT OR ANY INFORMATION HEREIN.

EXCEPT AS EXPRESSLY SET FORTH IN THE PARAGRAPH DIRECTLY BELOW, NO LICENSE IS GRANTED HEREIN, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS OF THE IOWN GLOBAL FORUM, ANY IOWN GLOBAL FORUM MEMBER OR ANY AFFILIATE OF ANY IOWN GLOBAL FORUM MEMBER. EXCEPT AS EXPRESSLY SET FORTH IN THE PARAGRAPH DIRECTLY BELOW, ALL RIGHTS IN THIS REFERENCE DOCUMENT ARE RESERVED.

A limited, non-exclusive, non-transferable, non-assignable, non-sublicensable license is hereby granted by IOWN Global Forum to you to copy, reproduce, and use this Reference Document for internal use only. You must retain this page and all proprietary rights notices in all copies you make of this Reference Document under this license grant.

THIS DOCUMENT IS AN APPROVED REFERENCE DOCUMENT AND IS SUBJECT TO THE REFERENCE DOCUMENT LICENSING COMMITMENTS OF THE MEMBERS OF THE IOWN GLOBAL FORUM PURSUANT TO THE IOWN GLOBAL FORUM INTELLECTUAL PROPERTY RIGHTS POLICY. A COPY OF THE IOWN GLOBAL FORUM INTELLECTUAL PROPERTY RIGHTS POLICY CAN BE OBTAINED BY COMPLETING THE FORM AT: www.iowngf.org/join-forum. USE OF THIS REFERENCE DOCUMENT IS SUBJECT TO THE LIMITED INTERNAL-USE ONLY LICENSE GRANTED ABOVE. IF YOU WOULD LIKE TO REQUEST A COPYRIGHT LICENSE THAT IS DIFFERENT FROM THE ONE GRANTED ABOVE (SUCH AS, BUT NOT LIMITED TO, A LICENSE TO TRANSLATE THIS REFERENCE DOCUMENT INTO ANOTHER LANGUAGE), PLEASE CONTACT US BY COMPLETING THE FORM AT: https://iowngf.org/contact-us/

Copyright © 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. Except for the limited internal-use only license set forth above, copying or other forms of reproduction and/or distribution of this Reference Document are strictly prohibited.

The IOWN GLOBAL FORUM mark and IOWN GLOBAL FORUM & Design logo are trademarks of Innovative Optical and Wireless Network Global Forum, Inc. in the United States and other countries. Unauthorized use is strictly prohibited. IOWN is a registered and unregistered trademark of Nippon Telegraph and Telephone Corporation in the United States, Japan, and other countries. Other names and brands appearing in this document may be claimed as the property of others.

Contents

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org

List of Figures

List of Tables

1. Introduction

Security risks are increasing year by year not only in terms of the problem of the increased frequency of cryptanalysis due to weakened cryptographic strength and the environment in which crimes are executed, such as providing criminals with RaaS（Ransomware-as-a-service）(Note1). In addition, in the era of the Innovative Optical and Wireless Network Global Forum (IOWN GF), attacks originating from within an organization, such as hijacking of official accounts, will become more common due to the spread of Artificial Intelligence (AI) technology. Methods such as taming internal parties through the proliferation of Social Networking Service (SNS) and exploitation using false boss instructions by Generative AI are good examples of such attacks. As a result, it is necessary to consider security measures that assume the intrusion is coming from the inside, and assurance of platform services alone is insufficient as a security measure. In the era of IOWN GF technologies, Zero Trust (in which users and devices should not be trusted by default) implementation that assumes intrusion is necessary, and services from service providers that support such implementation are necessary. The service provider providing applications based on the IOWN GF specifications should operate by prioritizing business continuity (minimizing damage and minimizing recovery), assuming that they will one day be compromised.

Platform service providers need to provide environment to realize application's business continuity operation, for example, by allowing applications to freely allocate encrypted areas.

Public key cryptography such as RSA and elliptic curve cryptography may be broken in a realistic amount of time by quantum computers. Platform service providers also need to increase cryptographic strength in order to cope with remarkable progress in practical usage of quantum computers.

1.1. Objectives

This document presents the IOWN GF's basic approach and policy on security as well as common requirements, including overlaps with security standards specified in ISO and other international standards. This document focuses on the technical areas defined in the IOWN GF and aims to clarify points to be considered in realizing the IOWN GF architecture.

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

Based on a Zero Trust approach, user data must be protected in all communications and computing, regardless of location.
In addition to external attackers, internal attackers at any location must be anticipated and the data to be protected must be encrypted at endpoints. An endpoint is an application process at the point where data to be protected is generated, processed or consumed. A user must also consider the risk of attackers inside the third-party service, regardless of whether it is trusted.

Additionally, the IOWN GF architecture data should be stored, exchanged, and computed according to policies specified by a data owner. Policies may include, but are not limited to, the following.

- Location: Data shall be located in the allowed country/company/organization as the policy specifies.
- Device: Data shall be sent/stored/computed using an appropriate device, e.g.., the chip vendor correctly produces the firmware and hardware of the device.
- Data access: Only authorized access is allowed as defined by policies.
- Computing function: The way data is processed is approved by the data owners through the policies.
- Controllability of disclosed data: Disclosed data is limited to processed information if the data owner so desires (e.g., anonymously processed information, statistical information, etc.).

(2) Achieve the post-quantum security

It has been pointed out that public key cryptography, 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 GF architecture needs to provide a means by which user data can be protected from attacks that utilize quantum computers.

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 used to protect the integrity of the information for data transfer.

(3) “Crypto-agility” to respond quickly and flexibly to new threats

While security against existing threats must be maintained, preparation against new threats to cryptographic algorithms is necessary, since it is unknown when and if cryptographic algorithms will be discovered to be vulnerable. It is desirable to increase “crypto-agility,” which is the ability of cryptosystems to respond quickly and flexibly to new threats, to prepare for possible future threats of cryptographic compromise. Conventional cryptographic protocols consist of vertically integrated key exchange functions, key management functions, encryption functions, etc. In such a configuration, if a new attack method is discovered and some of these functions are compromised, updating them without affecting other parts is difficult. Therefore, to achieve crypto-agility, it is necessary to have a disaggregation configuration that can flexibly update these functions.

(4) 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 the IOWN GF architecture, uniformly specify security measures and strengths is challenging. 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.

Multiple security measures and the ability to switch between them easily are also important requirements for responding quickly to future threats to data protection.

(5) Ensure compromise of 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 are consistent with the various performance requirements the IOWN infrastructure aims to achieve.

1.2. Scope

This reference document specifies the requirements and the functional security architecture for IOWN GF. In particular, the scope of this document includes:

- Common requirements for security
- Overview of security requirements for data in motion, data in use and data at rest
- Security functional requirements for platform implementation.

The details of security architectures are specified in the relevant architecture documents.

This document describes these three items in detail. However, to realize total security with IOWN GF, specific points should be considered in the application security architecture implementation. However, it is challenging to describe all the complex elements that require implementation in the IOWN GF platform. For this reason, the scope of the application security architecture described in the IOWN GF document is defined in the following three ways.

Scope of Application security described in the IOWN GF document

Applications must assign a class to each resource regarding business continuity (damage minimization and early recovery) in the business that the application embodies.
The application must be designed to provide security measures for each resource class and to handle notifications from monitoring to detect unknown intrusions.

Since these requirements are strongly application-dependent, the IOWN GF document assigns description contents and description documents in the following three types.

Type 1) When implementation dependency is high and it is difficult to define common resources as IOWN GF, these requirements shall not be described as requirements in the functional architecture document.

Type 2) When resources must be explicitly defined in IOWN GF use cases, describe the requirement as a use case document.

Type 3) When a user manual is created for application design, the requirement is described in the user manual.

2. IOWN GF Security Views

As mentioned above, it is necessary to provide IOWN GF defined services, e.g., network services and computing services, so that applications can be operated from the perspective of business continuity on the assumption that they will one day be penetrated. From a business continuity perspective, this means minimizing the direct damage to the business in the event of a partial attack on the environment in which the application is operated and minimizing the time it takes to recover from the damage. For this reason, the security view of IOWN GF, the perspective from which security is considered, needs to be functionally designed from the perspective of platform service application and the overall perspective of application operation. Specifically, the security requirements for IOWN GF defined services are organized by security view as follows:

1. Viewpoints on strengthening security through application operations considering possible threats that could remain in the IOWN GF defined service delivery platform.
2. Viewpoints for IOWN GF platform implementation
3. Viewpoints for security functions provided to the application

2.1. Viewpoints on strengthening security through application operations

” Viewpoints on strengthening security through application operations considering possible threats that could remain in the IOWN GF defined service delivery platform.” indicated in point 1 above. In a future where unknown attacks can penetrate internal and administrative systems, providing risk-free operation solely with Platform services is impossible. Security measures that are consistent across the board, including applications, are essential. For this reason, security is also considered one of the quality requirements, which are considered in light of ISO/IEC 25010 "Quality at the time of use" shown in Figure 2.1-1.

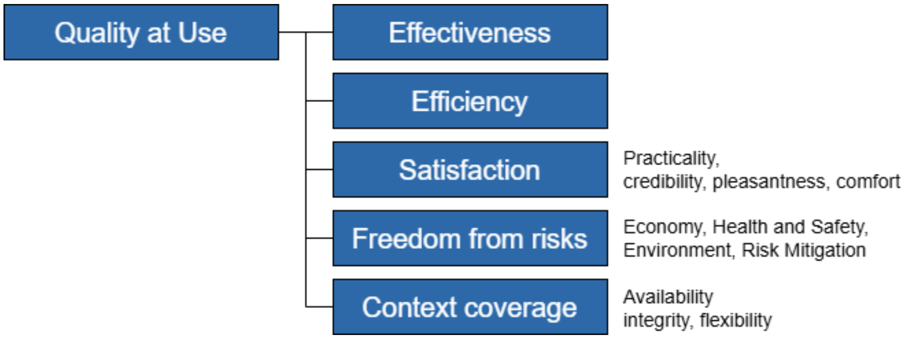


Figure 2.1-1: Quality in Use at ISO/IEC 25010

When considering application security measures from the viewpoint of business continuity , IOWN GF platform services must be equipped with monitoring and notification functions to detect unknown intrusions, minimize damage, and enable early recovery.

At the same time, applications must be designed internally to prioritize business continuity (damage minimization and early recovery), recognizing that IOWN GF platform services are not risk-free.

Therefore, IOWN GF platform services should provide flexible interfaces that allow free design of application operations.

A third-party organization should certify that the IOWN GF Platform Service is effective so that it can be used confidently.

2.2. Viewpoints for platform implementation

To clarify the viewpoint of platform implementation, this section contrasts the definition of information security between information systems that depend on platform implementation and information systems that are considered implementation-independent.

Platform-implementation-independent requirements are methodologies that provide direction for implementation, such as being based on the latest security design, providing resilience to unknown attacks, and monitoring and notifying unusual behavior for early recovery. Platform-implementation-independent requirements are presented in Chapter 5.

Table 2.2-1: Classification of information security

	INFORMATION SECURITY	
	Protection of information	Protection of information systems
Definition in this document	Protection of information is the protection of information that is used by or owned by the user of the IOWN infrastructure through the services defined by the IOWN GF. (NOTE 1)	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 1 - In the IOWN GF architecture, Protection of information includes not only protection in communication, but also protection of information during computing and during storage.

NOTE 2 - This document does not cover the details of commonly discussed technical aspects such as protecting personal information, handling of privacy, security risks and measures for hardware and software.

ITU-T and NIST Special Publication 800-12 define 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 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]

2.3. Viewpoints for security functionality provided to applications

From the business continuity perspective, advanced security services using cutting-edge technology are essential. Advanced security services enable applications to freely use isolated, secure areas, thus enabling flexible security design for applications. However, more is needed. Since data protection classes are designed by the application, the application must be able to freely assign data protection classes to its isolated secure area.

Moreover, even if the security is highly advanced using cutting-edge technology, a criminal's unknown attack could penetrate into the isolated safe area in the future. Therefore, it is necessary to monitor intrusions by unknown attacks in the platform using unusual behavior detection, etc., and to have a function that can detect unknown attacks early in preparation for such intrusions.

Detecting unusual behavior is not limited to "unknown attack detection mechanisms" already defined and known in each technical area. Detecting inconsistencies in the internal data of the platform service implementation system, detection of unusual frequency of accesses, etc., means monitoring to detect abnormal behavior that can be monitored within the implementation system in order to discover the possibility that it may be an unknown attack.

When an unknown attack (i.e., detection of unusual behavior) is detected, it should be reported to the application so that appropriate action can be taken according to the data protection class designed by the application.

Therefore, the three common security requirements for IOWN GF are as follows.

(1) Freely assign application data protection classes.

(2) Cutting-edge protection tech.--> providing secure areas.

(3) Monitoring for unknown attacks from inside or outside.

The IOWN GF should commonly provide security requirements to the application as shown in Figure 2.3-1.

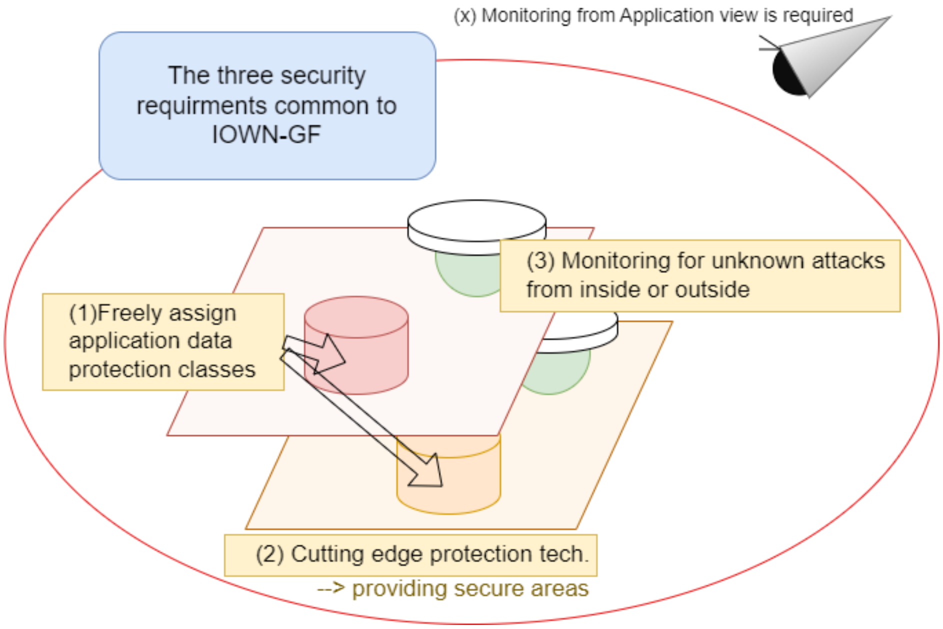

(x) Monitoring from Application view is required
The three security requirments common to IOWN-GF
(3) Monitoring for unknown attacks from inside or outside
(1)Freely assign application data protection classes
(2) Cutting edge protection tech.
--> providing secure areas

Figure 2.3-1: IOWN GF Security Service Requirement model

Note: The definition of resources to be protected depends on the application data protection class defined by the application, and the implementation of monitoring and reporting capabilities to detect unknown attacks depends on the platform implementation.
For this reason, this document describing IOWN GF security focuses on "(2) Cutting-edge protection tech.--> providing secure areas".
This document does not cover "(1) Freely assign application data protection classes" and "(3) Monitoring for unknown attacks from inside or outside".

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org

2.4. Zero trust model in IOWN GF

The three functions that should be provided to the applications described in the previous section are part of the Zero Trust model of IOWN GF. The Zero Trust model of IOWN GF focuses on minimizing the impact of applications on business in a Zero Trust environment where there is a possibility of intrusion by unknown attacks in the future. To achieve this, a model is adopted that maps critical resources to a secure, isolated area using cutting-edge technology provided by a service provider. By adopting this model, the application designs a data protection class, and the three functions that should be provided to the application to ensure its security are defined.
Now, the Zero Trust model of IOWN GF will be broken down in more detail.

As mentioned earlier, in the era of IOWN GF, it is necessary to design the system with a Zero Trust model that also considers attacks from inside the organization. This chapter describes the Zero Trust requirements from the perspective of the entire system, including applications C.f. [NIST SP-800 207].

Zero Trust models assume all devices and users possible to be compromised.
Thus in a Zero Trust design for business continuity, the top-layer applications must be designed minimizing business impact and speeding up business recovery in the event of an intrusion.

Figure 2.4-1 shows the relationship between the resources classified by the criticality of the applications to the business and the cutting-edge technology provided by the IOWN GF defined network services and computing services platforms.

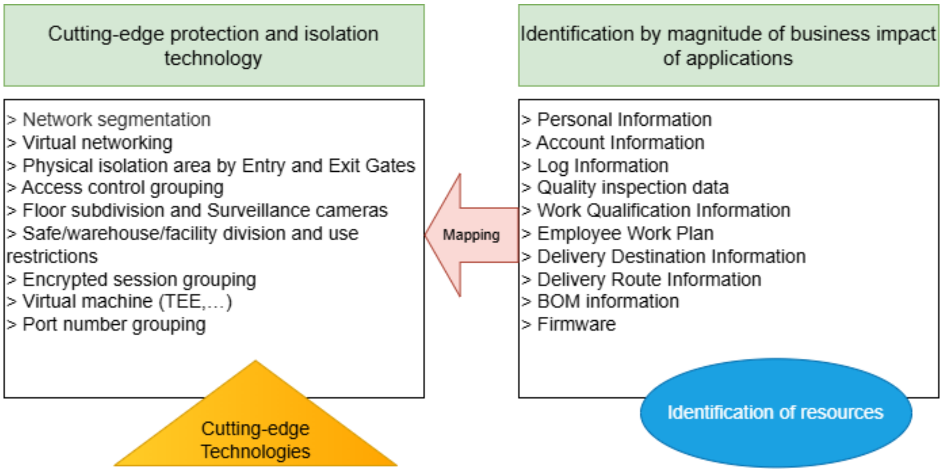

Cutting-edge protection and isolation technology
> Network segmentation
> Virtual networking
> Physical isolation area by Entry and Exit Gates
> Access control grouping
> Floor subdivision and Surveillance cameras
> Safe/warehouse/facility division and use restrictions
> Encrypted session grouping
> Virtual machine (TEE,…)
> Port number grouping
Cutting-edge Technologies
Mapping
Identification by magnitude of business impact of applications
> Personal Information
> Account Information
> Log Information
> Quality inspection data
> Work Qualification Information
> Employee Work Plan
> Delivery Destination Information
> Delivery Route Information
> BOM information
> Firmware
Identification of resources

Figure 2.4-1: Identification by the magnitude of the business impact of application and Cutting-edge protecting and isolation technology

In other words, IOWN GF's network service and computing service platforms provide “highly protected isolations of applications and systems using cutting-edge technology." Applications use isolated areas to appropriately divide and distribute and manage critical classified resources from their own business continuity perspective.
Such a security management model is shown in Figure 2.4-2 in contrast to the conventional perimeter model.

As mentioned above, the entire system, including applications, must be capable of early detection of unknown attacks, for example by monitoring and detecting abnormal behavior.

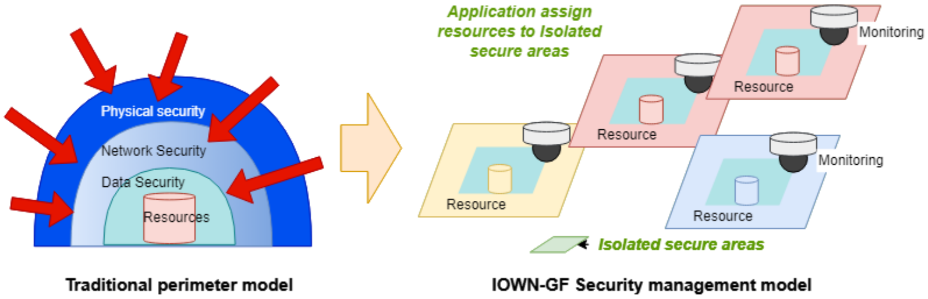


Figure 2.4-2: Security management model compared to the traditional perimeter model

2.5. Considerations in case the "end-to-end" service crosses an "external network"

There may be connection points to external networks other than the IOWN GF network.

If the application uses only IOWN GF network services, the security level will be the IOWN GF security level. If the “end-to-end” network service also includes (is composed of) an external network service, the overall security level could be lower.
The overall security level will be the lower than the IOWN GF security level or the external network security level.

Figure 2.5-1 shows an example of an external network service with a lower security level than the IOWN GF network service. In this case, the external network service is assumed to have no monitoring capability to detect unusual behavior against unknown attacks. In this case, the entire configuration shown in Figure 2.5-1 does not have functionality for detecting and monitoring unusual behavior targeting unknown attack detection. Therefore, in such a case, the level of security is lower than when using only IOWN GF network services.
Applications should be aware of the lower security level when such an external network service enters the system, and should consider, for example, refraining from transferring essential data over the route with the lower security level.

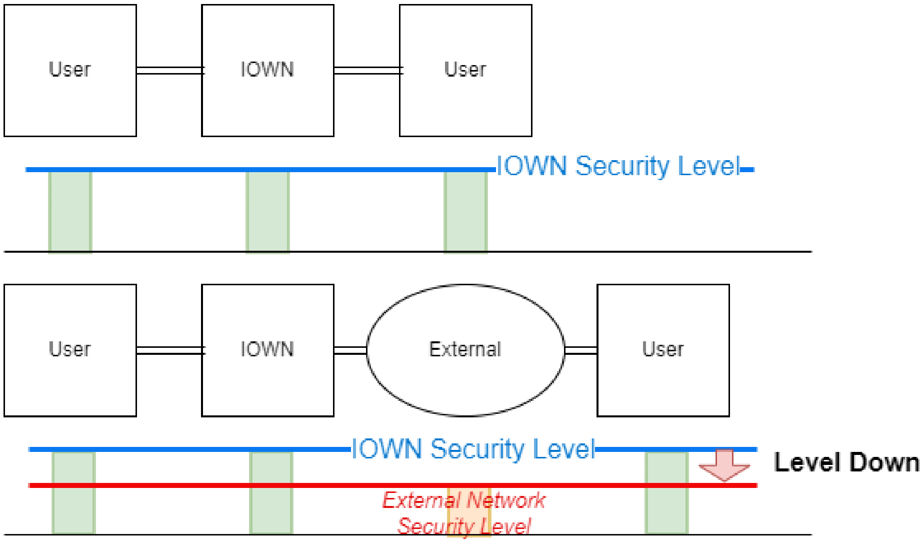


Figure 2.5-1: Example of the external network which has lower security level than IOWN GF

2.6. Interaction with IOWN GF infrastructure

The three security requirements common to the IOWN GF defined services described above are each related to other elements of the IOWN GF.

(1) Freely assign application data protection classes.
--> It relates to specific application implementations.

(2) Cutting-edge protection technologies.
--> providing secure areas.
--> Described in this document series of technology design.

(3) Monitoring for unknown attacks from inside or outside.
--> Provide monitoring functions within the platform to detect unknown attacks and report them to the application.
Monitoring for unknown attacks from inside and outside the platform is related to all elements of IOWN GF implementations.

3. Common Requirements for Security

3.1. Definition of security elements in IOWN GF

3.1.1. CIA (Confidentiality, Integrity, Availability)

In terms of security elements

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

- **Confidentiality**
    - Data in motion
      IOWN GF architecture should ensure the confidentiality of transferred data between the endpoints defined in section 1.1.
      User data information 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 third parties (e.g., service providers).
      When user data is transferred via a link in the IOWN GF architecture, it should be protected by appropriate security measures, such as data encryption and authentication of communication parties. Protection must be isolated for each user-directed unit, even for the same user.
    - Data in use
      The IOWN GF architecture should support the computation of data as well as its exchange and storage. Therefore, we need a mechanism that gives the security property including, but not limited to, the following.
        - Data confidentiality: Computation of data is done while keeping the data secret. In some cases, the output of the computation shall also be kept secret.
        - Algorithm confidentiality: The computation of data is done while the algorithm for the computation is kept secret.
    - Data at rest
      Highly confidential data must be able to be protected in accordance with user requirements by using encryption and/or secret dispersion technology. Protection must be isolated for each user-directed unit, even if it is the same user.
      A mechanism is required to monitor/detect/notify unauthorized access by obtaining data operation logs.
- **Data integrity**

The IOWN GF architecture must guarantee data integrity.
Appropriate control of users is also an important requirement for achieving “integrity”.
In addition, it is necessary to keep a history and be able to go back and review it. This will allow traces of errors and crimes to be tracked and corrected. While the backup enhancement will depend on the service definition, it is effective to have two copies and be able to detect differences by collation, or to be able to replace them in the event of loss or tampering.

- **Availability**

IOWN GF architecture should ensure the availability of its operation.

Expected availability measures are:

- Redundancy of systems such as 1: 1 or 1: n or m:n protection;

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org

- Ability to select an alternative data communication route.
- Proper backup of data
- Robust system operations (Continuous monitoring, failure prediction for proactive action, quick failure detection and rapid failover, etc.)

IOWN GF architecture should have capabilities for system resilience.

System 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. Resiliency is required for networking, processing, and storage, each of which must be combined to provide overall system resiliency.

When a security incident is detected, the resiliency capability should ensure that it is addressed in a controlled manner to minimize damage. In addition, it should ensure recovery of the system, restoring it at the required security level.

IOWN GF architecture should implement counter-measures against unknown attacks.

For example, network performance may be reduced (even to zero) due to DoS attacks on links. Appropriate methods could mitigate this issue, such as switching to backup links and rerouting data transfer.

3.1.2. Accountability, authenticity, reliability, and non-repudiation

Four important aspects of information security are Accountability, Authenticity, Reliability, and Non-repudiation.

- **Accountability**

Accountability is the ability to record and track who accessed information and by what procedure, etc. The IOWN GF architecture should ensure that records of security-critical actions are traceable uniquely to the functional elements that performed them.

IOWN GF architecture should support the traceability of data.

The dual functions of activity logging and security audits support these two security requirements.

Another possible but potentially weaker realization of accountability is achieved by the appropriate combinations of the authentication, access control, and audit trail functions.

IOWN GF architecture should be able to store information activities relevant to security in the IOWN GF architecture.

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

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

- **Authenticity**

Authenticity means ensuring that the person, device or software accessing the information is indeed an authorized user.

IOWN GF requires that, in addition to resource-based isolation, secure areas must also be available for authentication units designed by applications using two-step verification, multi-factor authentication, etc., based on the requirements of the aforementioned “1. User-free Resource Definition.”

- **Reliability**

Reliability refers to avoiding program and human errors and ensuring that the program operates and produces the intended results.

IOWN GF recommends that the system be able to monitor for signs of unknown attacks within it and report them to the application, based on the requirements of the aforementioned “3. Monitoring and Reporting.”

IOWN GF recommends the implementation of multi-factor security to prevent intrusion by attacks from a single security entity. (See 3.4. below)

- **Non-repudiation**

'Non-repudiation' refers to the retention of evidence so that the person responsible for a problem within the system cannot deny their involvement.

IOWN GF requires traceability, logs, audits, and predictive monitoring to ensure the above-mentioned “accountability” and “reliability”, and this also ensures “non-repudiation."

3.1.3. Security requirement for information assets to be protected

As described in 3.1 above, information assets to be protected are defined from a business continuity perspective because the IOWN GF security model adopts the most advanced Zero Trust model.

The information assets to be protected are defined from the Service Provider's perspective regarding its platform services, and the application perspective regarding applications built on the IOWN GF.

The IOWN GF defined service provides an environment where applications can freely define the information assets to be protected.
The definition of information assets to be protected by the IOWN GF-defined service itself is implementation-dependent and is not discussed in detail in this document. Therefore, the information assets to be protected shown in this document should be considered as the information assets to be protected defined by the application, which is freely designed by the application in terms of importance unless otherwise specified.

For example, in the case of protecting Data-in-Motion, the information assets to be protected are the information assets that the application has defined as important. From the perspective of the IOWN GF service provider, it can only be recognized as a part of the user data handled by the endpoint in end-to-end communication. Therefore, it must be an environment where the application can selectively invoke the communication that includes the information assets to be protected and isolate them for security.
For this reason, the threat analysis in this paper is limited to a scope that does not extend to implementation. For example, in protecting Data-in-Motion, the threats in E2E communication are described at the abstraction level of the reference model.

The reference implementation model considered in IOWN GF can be cited as an example of concrete assets that need to be protected.

3.2. Security requirement level

3.2.1. 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 **known** 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.

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org

IOWN GF requires level 2 or higher security against computer attacks.

3.2.2. Security against third-party attacks

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, which are 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 an excellent 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 information protection. At this level, the users can establish secure end-to-end communication, or store data without fear of third-party attacks. It must also have monitoring and detection functions for unknown attacks.

IOWN GF requires level 2 security against attacks from third parties.

3.3. MFS (Multi-Factor Security)

3.3.1. 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 achieved with a single method.

There are two types of Multi-Factor Security (MFS) techniques, both of which achieve a level of security that cannot be achieved with a single technique

1. Combination (Technology to increase security strength)
   By combining different types of security elements, attacks on a single security entity are prevented from breaching the system.
2. Switch (Technologies to Increase Security Resilience)
   Switch ensures recovery agility by quickly switching between different types of security elements.

A well-known example of MFS is multi-factor authentication (MFA) where different authentication factors are combined to counter different security threats. IOWN GF recommends the implementation of multi-factor security to prevent intrusions caused by attacks on a single security factor.

3.3.2. Multi-Factor Security for IOWNsec

IOWNsec multi-factor security is a common technology that can be selected in all cases, not just for communication (data in motion), but also for computing (data in use) and storage (data at rest). Combining multiple security methods frustrates attackers and provides more robust security.

Please refer to the functional architecture documents for each multi-factor security technology. Here, to understand the concept, a case study of key exchange for communication is outlined to articulate the concept.

It would be beneficial to combine the key exchange methods shown in Figure 3.3-1, which involve a third-party service provider from the endpoint's perspective (Type-A), with the key exchange method that only consists of the

sender and receiver as endpoints (Type-B).
The combination of Type-A, which is robust encryption method despite the threat posed by third-party service providers, and Type-B, which is a less strong encryption method between endpoints without the involvement of a third party, provides a combination of key exchanges from different threat points, and can provide more robust security.

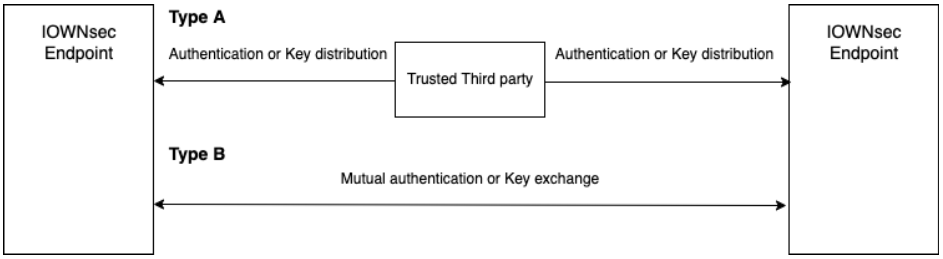

IOWNsec Endpoint
Type A
Authentication or Key distribution
Trusted Third party
Authentication or Key distribution
IOWNsec Endpoint
Type B
Mutual authentication or Key exchange

Figure 3.3-1: Difference between Type A and Type B

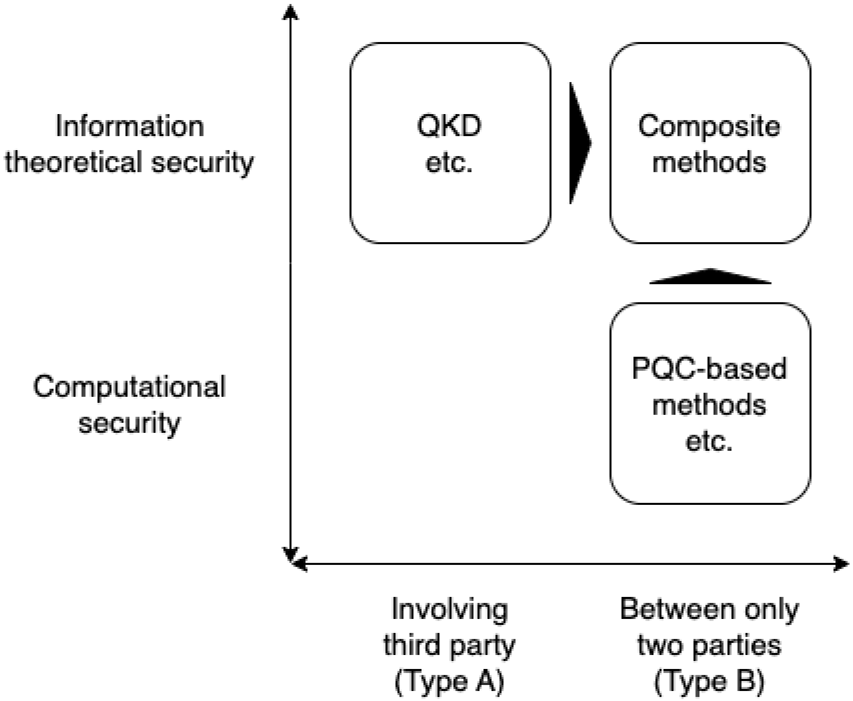

Information theoretical security
Computational security
QKD etc.
Composite methods
PQC-based methods etc.
Involving third party (Type A)
Between only two parties (Type B)

Figure 3.3-2: Image of the impact of combining Type A and Type B

Assuming that both strengths of both are maintained in the MFS for key exchange, the effectiveness of combining Type-A and Type-B can be understood as shown in Figure 3.3-2. For more details, please refer to the Functional Architecture Document.

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, several post-quantum cryptographic algorithms have been proposed, including lattice-based cryptographic algorithms, code-based cryptographic algorithms, multivariate cryptographic algorithms, hash-based signatures, and others.

3.4. Authentication and access control

An authentication function should establish identifiers and verify the claimed identities and any other entities if these are connected to the IOWN GF 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 that are connected to the IOWN infrastructure;

Entity authentication: establishes the proof of the identity of the functional elements in the IOWN infrastructure 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 data confidentiality. They ensure that only authorized parties can access the data, and that it is integrity-and authentic.

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

IOWN security 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.

3.5. Dynamic defense

Zero Trust captures dynamic defenses in a way that is counter to perimeter defenses.
Perimeter defenses, they rely on implicit trust. Once one enters a certain bounded trust zone through authentication and authorization, all subsequent resource requests are also assumed to be valid.
In dynamic defense, the focus should be reducing authentication, authorization, and implicit trust zones to reduce uncertainty.

The availability of authentication mechanisms must be maintained, and time delays must be minimized.
The IOWN GF architecture must develop and maintain dynamic, risk-based policies for resource access and build a system that ensures these policies are correctly and consistently enforced for individual resource access requests. In other words, the IOWN GF architecture should not rely on implicit trust, whereby if an entity satisfies a basic level of authentication (e.g., login to an asset), it is assumed that all subsequent resource requests are equally valid.

3.6. Intrusion detection

The IOWN GF system must be implemented according to a Zero Trust model.
Assets are inherently untrusted. The IOWN GF architecture takes into account the security posture of assets when evaluating requests for resources.

Continuous diagnostics and mitigation must be established and operational to monitor device and application status. In other words, a robust monitoring and reporting system is required.

Methods for monitoring device and application status are highly implementation-dependent and not always unambiguously right/wrong. One method of device and application state monitoring is to monitor for and detect early intrusion into the system due to unknown attacks, e.g., by detecting unusual behavior, just as a security operations center attempts to detect unusual behavior.
Detection of inconsistencies in the internal data of the platform service implementation system, detection of unusual access frequency, etc. It is up to the Service Provider to what extent to implement detection of unusual behavior that can be monitored within the implementation system.
If an unknown attack (detection of unusual behavior) is detected, it should be reported to the application so that the application can take appropriate action according to the data protection class for which it was designed.

4. Overview of Security Functional Requirements

4.1. Common reference model for data in motion, in use, and at rest

This section describes the data security reference model for communication, computing, and storage containment. As shown in the Figure 4.1-1, there are three main categories of locations where data should be protected.

Data in motion

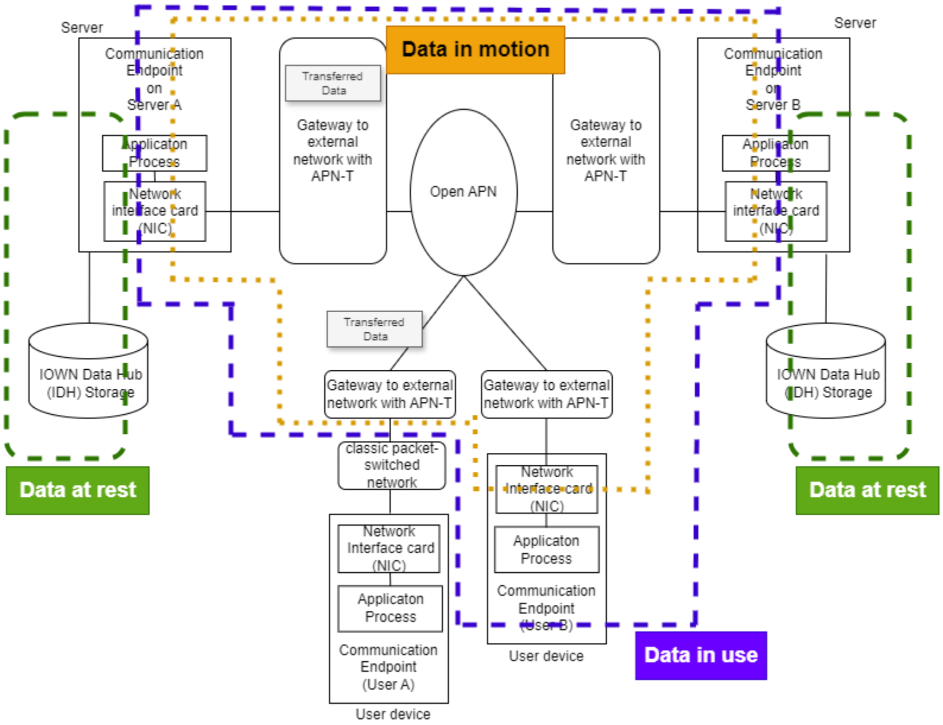
Data in motion is data in transit between IOWNsec endpoints or within computer systems.

Data in use

Data in use is data that is currently being processed by IOWNsec endpoints. Because the IOWN infrastructure enables distributed and heterogeneous computing, this document defines data in use in a broader scope that includes data in motion.

Data at rest

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



Server
Communication Endpoint on Server A
Applicaton Process
Network interface card (NIC)
IOWN Data Hub (IDH) Storage
Data at rest
Transferred Data
Gateway to external network with APN-T
Data in motion
Open APN
Gateway to external network with APN-T
Server
Communication Endpoint on Server B
Applicaton Process
Network interface card (NIC)
IOWN Data Hub (IDH) Storage
Data at rest
Transferred Data
Gateway to external network with APN-T
Gateway to external network with APN-T
classic packet-switched network
Network Interface card (NIC)
Applicaton Process
Communication Endpoint (User A)
User device
Network Interface card (NIC)
Applicaton Process
Communication Endpoint (User B)
User device
Data in use

Note) Data that are not represented in this diagram, including data that is not considered to be protected, are classified into one of these three types when they are to be protected.

Figure 4.1-1: Reference Model of IOWN Security

4.2. Data in motion

Data in motion refers to digital information actively moving from one location to another. This is used to process and analyze big data in real or near real-time [NIST Special Publication 1500-1]. This information that flows in data in motion contains a lot of confidential information as a company. Thus, it is crucial to protect this information.

4.2.1. Threats for data in motion

Security threats at "Data in Motion" are everywhere. In this section, consider the architecture of IOWN GF and the issues that need to be focused on because this is the era in which it will be applied.

The main threat that should be considered is the threat of a malicious third party using the capabilities of a quantum computer to perform cryptanalysis and infiltrate the internal network.

4.2.2. Existing technologies

4.2.2.1. Authentication and authorization

This section introduces existing technologies for authentication and authorization.

DSA, ECDSA, EdDSA and RSA are used for authentication using SSH public key cryptography. Digital signatures are used to detect unauthorized modifications to data and to authenticate the signatory’s identity. In addition, the recipient of signed data can use a digital signature as evidence for a third party. (excepts from the abstract of the [NIST FIPS 186-4]) DSA, ECDSA, EdDSA, and RSA are based on mathematical problems that are difficult to solve. However, some new quantum computer algorithms will soon solve some of the above mathematical problems in real-time. The digital signature algorithms for authentication can be found in [NIST SP 800-131A Rev. 2].

PQC (Post-quantum cryptography) based digital signature has been proposed to prevent quantum computer decryption. PQC uses cryptographic algorithms based on mathematical problems that are difficult to solve by a quantum computer. PQC is easy to install in a variety of information systems. However, some algorithms may have to be improved as computers and their capabilities evolve. The selected digital signature algorithm of NIST's PQC standardization can be found here. [NIST PQC Selected Algorithms 2022]

PSK (Pre-shared key) based digital signature has been also proposed. A pre-shared key is a secret key established between the parties authorized to use it through some secure method [NIST SP 800-133 Rev. 2]. Set a shared key for multiple devices and check for a match when authenticating. It is quantum-resistant technology under certain conditions. However, this approach consumes resources, especially with the continued rotation of keys. 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.

4.2.2.2. Key exchange

Existing public key cryptography–based key exchange methods including Diffie-Hellman and RSA are regarded as secure, because they involve complex mathematical problems that take a long time to solve with non-quantum computers. However, some new quantum computer algorithms can solve some of the above mathematical problems in real-time. Therefore, the existing key exchange methods are no longer secure in a quantum computing era.

Key establishment methods that utilize PQC as described in the Authentication section is alternative approach in the quantum computing era. They are considered secure because they use cryptographic algorithms based on mathematical problems that are difficult for a quantum computer to solve. The selected key establishment algorithm of NIST's PQC standardization can be found here [NIST PQC Selected Algorithms 2022].

QKD (Quantum Key Distribution) is another approach for the key exchange. It produces and distributes the keys whose security relies on quantum mechanics theory, in opposition to classical public and PQC cryptography, which is based on computational difficulty. The eavesdropping by a third party unavoidably introduces errors to the system through additional noise, based on the principle that the measurement of quantum states itself causes disturbances to the states. The legitimate parties can detect such hacking attempts by detecting defined threshold of errors, and then discard the corresponding quantum states that are not used to produce the key. However, QKD networks frequently require trusted relays, entailing additional costs for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.

4.2.2.3. Encryption

The Advanced Encryption Standard (AES) cryptographic algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) data in blocks of 128 bits with cryptographic keys of 128, 192, and 256 bits [NIST FIPS 197]. 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 challenging to find a key to decrypt data as it is today.

As an alternative approach, one-time pad (OTP) is a system in which a randomly generated private key is used only once to encrypt a message, which the receiver then decrypts using a matching OTP and key. Because of its information-theoretic security, OTP is recommended to ensure the long-term confidentiality of keys. However, since it is a stream cipher, it requires a large number of pre-shared keys the same size as the data being exchanged.

4.2.3. Technology gaps

Various quantum-resistant authentication, key exchange, and encryptions have been proposed, but none of them are absolutely safe. Therefore, the MFS concept as described in Section 3.3 is significant.

In the PQC based method, a hybrid method has been proposed in which a combination of a conventional cryptographic algorithm and a secure algorithm is used to raise the security level that can withstand a quantum computer. [IETF Hybrid key exchange in TLS 1.3 2024] In addition, crypto-agility has been proposed to replace compromised key exchange method with secure key exchange methods. [NIST Getting Ready for Post-Quantum Cryptography 2021]

For authentication, the MFS concept can be implemented using specifications defined by other SDOs. However, key exchange cannot be achieved by existing specifications alone. Both key exchange and encryption must be considered to realize the MFS concept. To promote conceptual understanding of the MFS concept, a case study of key exchange for cryptographic communication was outlined in Section 3.3. The first option of MFS key exchange and management concept is to combine different types of key exchange methods to address a wider range of threats. Another option is to be able to quickly switch key exchange algorithms, thereby preparing for future algorithmic compromises. Communication must continue even if key exchange methods are combined or switched. This requires a mechanism to store and switch keys between them. In addition, data in motion also handles large volumes of data and is processed in real time as shown in 4.1. In these cases, data encryption is offloaded to the operating system or physical hardware. There is currently no architecture for switching and combining of key exchange in such a configuration. Therefore, In IOWNsec, MFS key exchange and management was proposed to achieve multi-vendor quantum-resistant key exchange and encryption.

4.2.4. Direction to fill gaps - MFS key exchange and management

The basic concept of MFS key exchange and management is shown in Figure 4.2-1. The encryption keys for cryptographic communication are generated by combining keys from different key exchange methods and are supplied to the cryptographic application synchronously between IOWNsec endpoints through "Key management". These key exchange methods can be switched at arbitrary times. By combining and switching between multiple key exchange methods, secure communication can always be maintained even if one of the key exchange schemes is suddenly compromised.

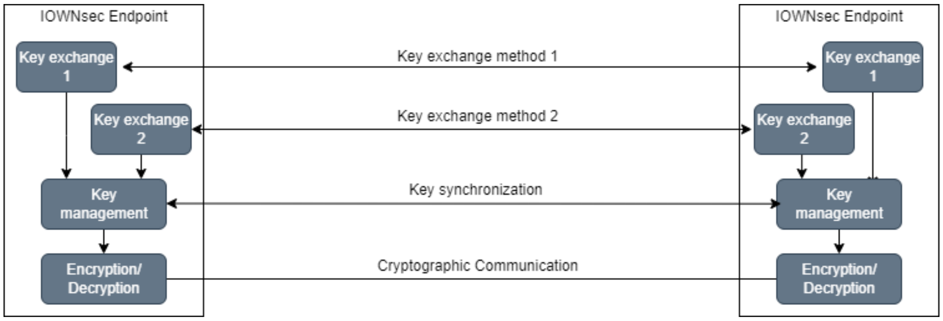


Figure 4.2-1: Basic concept of MFS key exchange and management

Figure 4.2-2 shows a hierarchical structure of the MFS key exchange and management. MFS key exchange layer provides key exchange between two nodes. MFS key management layer provides key synchronization between two nodes, as well as key combining and key update management on the nodes. Cryptographic communication layer provides encryption/decryption functions for secure data communication between two nodes. This structure enables layer-by-layer development and reduces development time. It also provides cryptographic agility and zero-trust security through the flexibility of changing cryptographic communications. The MFS key exchange and management architecture is defined in another document.

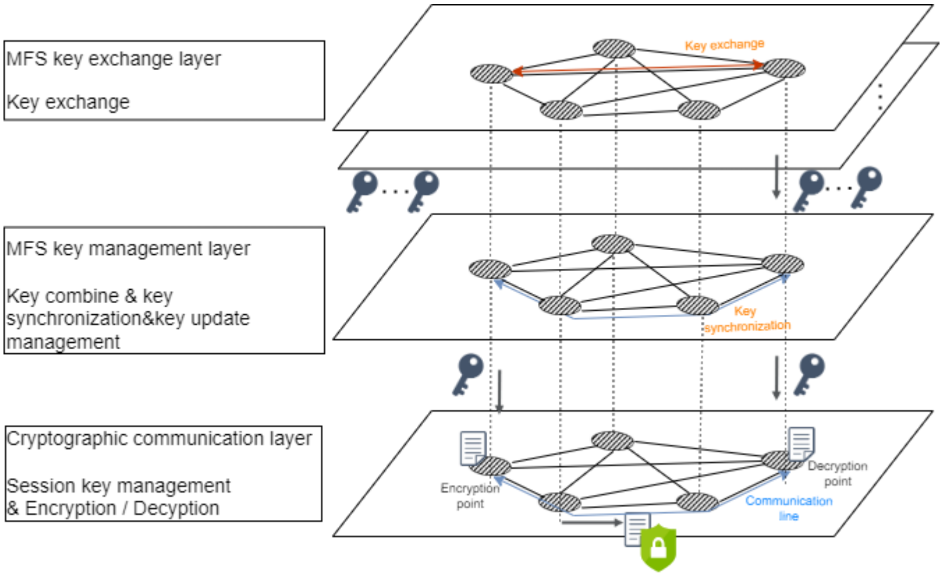


Figure 4.2-2: Hierarchical structure of the MFS key exchange and management

4.3. Data in Use

4.3.1. Privacy-Enhancing Technologies for protection of data in use

Open data distribution schemes are gaining momentum as a global trend, as seen in the International Data Space Association (IDSA) and Catena-X [IDSA] [Catena-X]. However, although today's data distribution schemes define conditions for data handling, such as policies for data access control, they do not provide technical guarantees for the protection of the data itself for its lifetime, e.g. data can be distributed to the place where is not allowed by policies once it has been acquired by authorized users. Most regulations on data distribution between entities only specify the protection of data in motion and data at rest, and do not provide technical guarantees on how data is protected once it has been passed.

As described above, from the data owner's perspective, data distribution needs to be based on mutual trust between the data owner and data user that contracts are honored. This means that data distribution is currently not at a stage where the owner can provide their data with confidence. As a promising solution for protecting data in use, privacy-enhancing technologies (PETs), a generic term for technologies that enhance privacy protection including confidential computing has been attracting attention in recent years. In the OECD report [EMERGING PRIVACY ENHANCING TECHNOLOGIES], it is said “PETs are promising because they expand access to data analytics while increasing digital security and privacy and data protection. For example, PETs support collaborative analysis over data that would otherwise be too sensitive to disclose, combine and use across individuals or entities.”

IOWN GF focuses on PETs as a solution for protection of data in use.

4.3.2. Threats for data in use

The following data security threats exist on current data distribution platforms.

- Data use that is not compliant with agreed-upon usage policies between the data provider and the user: Users with data access rights or privileged users of the shared infrastructure use data beyond the agreed scope in violation of policies.
- Malicious data attacks within the shared infrastructure: Information is compromised when external attackers break into virtual machines or underlying hypervisors (so-called Dom0 VMs) or when insider attackers exist in the shared infrastructure and have access to protected data.

4.3.3. Existing technologies

In the OECD report, the PETs are divided into the following four broad categories: (i) data obfuscation, (ii) encrypted data processing, (iii) federated and distributed analytics, and (iv) data accountability tools. The first three, which can directly protect data, are highlighted here.

4.3.3.1. Data obfuscation

Anonymization: Anonymization is the process of removing identifying elements from data to prevent re-identification of the data subject. Anonymized data, therefore, should in theory not be linkable back to an individual even when combined with additional data sets.

Differential privacy: Differential Privacy is a mathematical framework that enables the publication of statistical information about a data set while protecting the privacy of individual data in functions such as data publication, data analysis, etc. It typically reduces the privacy risk by adding Gaussian or Laplacian noise to the function, selected to make it unable to infer any individuals in the dataset.

4.3.3.2. Encrypted data processing

Secret Sharing-based Multi-Party Computation (SS-MPC): Secret sharing (SS) is a cryptographic technique used to protect the confidentiality of a message by dividing it into pieces called shares. In SS-MPC, a message is shared among participating parties via SS, and the parties compute a function on the shared message while maintaining its confidentiality and obtaining shares of the function output. The output can be obtained using a message reconstruction algorithm of SS, taking all or a subset of the output shares as input.

Homomorphic Encryption (HE): HE is a type of encryption in which addition, multiplication, or a combination of these can be performed while encrypted. One promising application is outsourcing computation, where cipher texts are handed over to a third party and the computation is performed by that party.

Trusted Execution Environment (TEE): The TEE is a secure area within a processor. It guarantees that the code and data loaded inside it are protected with respect to confidentiality and integrity. Essentially, TEEs provide a kind of ‘safe room’ for sensitive operations, ensuring that even if a system is compromised, the data within the TEE remains secure. TEEs operate by isolating specific computations, data, or both, from the rest of the device or network. This isolation is hardware-based, which makes it highly resistant to external attacks, including those from the operating system itself. Within a TEE, code can run without risk of interference or snooping from other processes [TEE].

4.3.3.3. Federated and distributed analytics

Federated Learning: Federated learning (FL) is a distributed Machine Learning (ML) approach that trains ML models on distributed datasets. The goal of FL is to improve the accuracy of ML models by using more data while preserving the privacy and the locality of distributed datasets. FL increases the amount of data available for training ML models, especially data associated with rare and new events, resulting in a more general ML model [FL].

4.3.4. Technology gaps

Regarding data confidentiality, technologies to protect data in use are becoming increasingly used in actual services, but they do not cover data protection when transitioning between states. In Disaggregated Computing in the IOWN era, data owners are assumed to combine distributed resources on demand to handle live data. In such an era, the conventional access model, in which data is collected and then authorization is set in a centralized manner, cannot fully protect data. Therefore, it is important to define policies that govern how data is handled when it is generated and have a mechanism to enforce them when the data is distributed. In addition, to prevent data siloing and realize active data distribution across organizations and countries, it is necessary to realize the above data protection mechanisms using open interfaces that do not depend on specific vendors or operators. Although there are many existing technologies to protect data in use, as described above, no mechanism that enables seamless protection of the entire data lifecycle and simultaneous data usage control has been realized for open data collaboration.

4.3.5. Direction to fill gaps - IOWN Privacy-Enhancing Technologies

IOWN GF focuses on PETs, which can be a generic solution as technologies to protect data in use and proposes an architecture called IOWN Privacy-Enhancing Technologies (IOWN PETs) that seamlessly connects technologies that protect data in each state and simultaneously enables policy-driven data usage management to maintain confidentiality and data sovereignty throughout the entire data lifecycle in order to promote active data distribution on the IOWN infrastructure.

IOWN PETs is defined as a common platform layer that provides secure virtual spaces in which data confidentiality and governance are technically guaranteed throughout the data lifecycle in accordance with policy using IOWN infrastructure such as APN and DCI.

The IOWN PETs architecture is defined in another document.

4.4. Data at rest

4.4.1. Threats for data at rest

The confidentiality and integrity of data stored in storage infrastructure must be secure against attacks from malicious attackers. At the same time, ensuring availability is also important for users' convenience. Depending on the attributes of stored data, some data that require long-term confidentiality and integrity (medical data, etc.) and data require short-term confidentiality and integrity (some system data, etc.), and security requirements vary. Affordable measures are required to consider these security requirements.

Among the data stored in storage, data that needs to be stored for a long time is required to be disaster-resistant and fault-resistant (i.e. availability) so that even if part of the data is lost due to natural disasters such as earthquakes and typhoons or server failures, the original data can be restored. For this purpose, security measures to divide and/or duplicate data and store it in geographically distributed servers are helpful. Still, at the same time, security risk arises when part of the distributed data is disclosed or lost. Therefore, security measures are required to assure the confidentiality of the original data even if it is divided and/or duplicated.

4.4.2. Existing technologies

This section introduces existing technologies for the protection of data at rest.

Backup of data is the creation of a copy of data in order to restore the data to a specific point in time. The data to be stored can be either a copy of all of the data or a copy of the differences from a specific point in time. From the copy created, the data can be restored to a specific point in time of the event that causes file corruption, system failure or data loss. The server that backs up the data can be on-premises, on-cloud, or in other configurations. Backing up data may take a long time, and if so, backups are usually scheduled overnight to reduce the impact on the system.

Data replication is the process of creating one or more copies of data, and distributing them across multiple storages. It can be either synchronous (performed in real-time) or asynchronous (performed on a schedule). In synchronous replication, the entire system is replicated first, and then data changes are captured and written to the remote storages at the same time as the primary storage. In the event of a disaster or failure, failover to the secondary replication site is almost instantaneous.

Secret sharing is one of the security measures to protect the confidentiality, integrity and availability of data at rest. Secret sharing creates multiple data pieces (shares) from the original data using a polynomial and storing them in multiple data servers (shareholders). Five secret sharing schemes are standardized in ISO/IEC 19592-1 and 19592. Shamir’s secret sharing scheme (Shamir's (*k, n*) threshold scheme) is one of them. It uses n shareholders and restores the original data by collecting at least *k* (≤*n*) of shares. With *k*–1 or fewer shares, the original data can never be reconstructed even with unlimited computing power. Provided that the number of corrupted shareholders is less than k, and shares are exchanged through private channels, Shamir's (*k, n*) threshold scheme ensures information theoretic confidentiality of storage that is, confidentiality is satisfied. Even if shares up to *n*–*k* are lost, the original data can be reconstructed using the k remaining shares, which provides availability. The confidentiality and integrity of data transferred between shareholders should be protected by appropriate security measures such as encryption.

4.4.3. Technology gaps

Data does not necessarily need to be encrypted and stored if the storage is accommodated in a trusted place (e.g., physically protected). However, to guarantee the confidentiality and integrity of the stored data for the long term, it is desirable to encrypt data with highly secure methods (i.e. PQC, OTP with the key provided by QKDN) and periodically renew the encrypted data. If data is encrypted and stored, the encrypted data and the key used for encryption must be stored securely. When data is encrypted and stored in a centralized (single) server, it is possible to protect the confidentiality and integrity of the data, but the risk of losing the data due to disasters or failures of the server cannot be avoided. When data is encrypted and stored in distributed (multiple) servers, the risk of compromising the confidentiality of the data increases. There is a need for technologies that protect the confidentiality and integrity of data while ensuring resilience to disasters and system failures. Considering resilience to disasters and system failures, storing data in geographically distributed storage infrastructure is desirable. However, instantaneously transferring data among geographically distributed storages locations, and performing large-scale backups in real-time might be difficult with existing network technologies.

4.4.4. Direction to fill gaps

For the protection of data at rest within the IOWN GF implementation, an architecture can leverage an Open APN to protect backup and replicated data in the distributed storage locations instantaneously. For this purpose, it is necessary to study security techniques and combining encryption methods using MFS architecture including PQC and QKD against threats posed by quantum computers between the distributed storage locations.

NOTE - Security methods for protecting data at rest in IOWN GF need further study.

5. Security Functional Requirements for Platform Implementation

As described in Section 2.2, "Security Requirements for Platform Implementation," this document does not define in detail the security requirements for platform implementation in detail. These requirements are highly implementation-dependent. We expect service providers to implement based on the Zero Trust concept. In other words, service providers are expected to implement based on the latest security design based on regulations and methodologies defined by global standards bodies such as ISO and NIST.

In applying security measures based on business impact estimation in the event of an unknown attack, providers are expected not only to consider their own business impact, but also to implement security measures in a manner that allows users to freely control security measures according to the magnitude of the business impact of the users of their services.

In addition, to promote early recovery from unknown attacks together with users, please be sure to implement a real-time monitoring mechanism within the provider's platform. Report any "unusual behavior" detected in a meaningful way to the user and in a user-reactionable manner.

Security regulations often vary from country to country and industry to industry, and IOWN providers with users in multiple countries and industries are expected to be flexible in their implementation.

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org

6. Differences in Concepts with General Security Standards.

This document describes cutting-edge security technologies that can address various security risks in the IOWN era, how to provide them on the IOWN platform and methods for building applications on that platform. It is based on the latest security designs and does not contradict the regulations and methods set forth by ISO, NIST, and other global standards organizations.

The security measures prescribed by the latest global standards bodies recommend implementing Zero Trust (assuming intrusion) to counter evolving attacks. In other words, they encourage security measures that focus on business continuity. The security measures in this document are consistent with this direction. The description in this document is focused on IOWN GF and concentrates on points that both providers and users of IOWN GF-defined services should consider.

To respond to the risks of the IOWN era, the document focuses on the cutting-edge technologies such as MFS and PETS that deserve special mention. It also provides considerations for application design, but unfortunately, it does not address implementation.

It is evident that security measures cannot be materialized without addressing the implementation level, since the business impact differs depending on each system, business, country, etc. However, please understand that the IOWN GF document does not break down to that level.

References

[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

[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 800-207] 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

[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 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 Special Publication 1500-1]NIST Special Publication 1500-1,NIST Big Data Interoperability Framework: Volume 1, Definitions, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf

[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 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 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 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 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

[IETF Hybrid key exchange in TLS 1.3 2024]IETF, Hybrid key exchange in TLS 1.3, draft-ietf-tls-hybrid-design-11, 7 October 2024, https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/11/

[NIST Getting Ready for Post-Quantum Cryptography 2021]NIST Cybersecurity White Paper, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, April 28, 2021 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

[IDSA]https://internationaldataspaces.org

[Catena-X]https://catena-x.net/en/

[EMERGING PRIVACY ENHANCING TECHNOLOGIES]EMERGING PRIVACY ENHANCING TECHNOLOGIES, CURRENT REGULATORY AND POLICY APPROACHES, OECD DIGITAL ECONOMY PAPERS, March 2023 No. 351, https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html

[TEE]Confidential Computing Consortium, “Basics of Trusted Execution Environments (TEEs): The Heart of Confidential Computing – Confidential Computing Consortium”, 2018.

[FL]AWS, Reinventing a cloud-native federated learning architecture on AWS, https://aws.amazon.com/jp/blogs/machine-learning/reinventing-a-cloud-native-federated-learning-architecture-on-aws/

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org

History

REVISION	RELEASE DATE	SUMMARY OF CHANGES
1.0	February 15, 2023	Initial Release
2.0	February 05, 2025	While the scope of Release 1 was the protection of data in motion, Release 2 was completely restructured to include the following items. -Common requirements for overall security to be considered in the IOWN Global Forum. -In addition to the protection of data in motion, functional requirements for the protection of data in use and data at rest to be considered in the IOWN Global Forum. The details about protection of data in motion described in Release 1 moved to the Functional Architecture for Protection of Data in Motion.

© 2025 Innovative Optical Wireless Network Global Forum, Inc. All rights reserved. • www.iowngf.org