IOWN GLOBAL FORUM ™

Multi-Factor Security (MFS) PoC Reference

Classification: APPROVED REFERENCE DOCUMENT

Confidentiality: PUBLIC

Version 1

October 2023

[MFS PoC Reference]

Legal

Contents

List of Figures

1. Introduction

1.1. Purpose

The goal of IOWN GF is to develop new fundamental technologies to improve communication, computing, and energy efficiency. Security for IOWN communication and storage is vital to support future ICT infrastructure. In order to secure transferring and storing data of IOWN GF systems, appropriate security solutions are required against threats which are derived by quantum computers. In March 2023, IOWN GF proposed Multi-Factor Security (MFS) [IOWN GF SEC OUTLOOK] as a post quantum security architecture for data communications. The purpose of this PoC is to clarify the impact of MFS on the performance of data communication over Open APN.

1.2. Objectives

There are many possible implementation patterns for MFS. Accordingly, the objectives of this PoC are to:

- gather performance values for specific examples of MFS for clarifying the impact of MFS on IOWN communications,
- gather best practices for implementation of MFS.

1.3. Scope

This PoC aims to verify the impact of MFS, which provides communication security, on communication performance compared to the case without encryption or to the currently commonly used key exchange and encryption method. Accordingly, PoCs do not need present complete or even partial use-case applications since that would be the scope of reference implementation model (RIM) PoCs. This PoC reference outlines the validation perspectives for evaluating the performance of MFS, and PoC reports should report the maximum impact on communication performance for each validated implementation, so that service providers using MFS can understand the impact on communication performance.

2. Example Reference Cases

This section touches on several possible use cases for MFS to provide readers with positioning of KPIs and performance value criteria.

Data center exchange

These reference cases utilize IOWN infrastructure to solve environmental problems such as shortages of land and electricity in urban areas and carbon dioxide reduction, as well as inefficiency and high costs due to distributed data center placement. Specifically, the following use cases are conceivable for virtually integrating data centers by exchanging data between data centers in different locations at high speed, large capacity, and low latency. Examples of use cases:

1. Communication between urban data centers and annex data centers in outskirts (assumed users: OTT players, organizations with AI centers)
2. Public cloud interconnect communication (assumed users: public/financial sectors)
3. Communication between on-premises and cloud environment (assumed users: financial, retail, manufacturing, governments)
4. Communication between edge computing environment and cloud environment (assumed users: MEC customers, e.g., mobility companies)

- Assumed key performance requirements related to MFS
  - RTT: Less than 1-2 ms
  - Bandwidth: Several hundred Gbps ~ several Tbps
  - Other requirements that may be related to MFS (e.g., Jitter, Packet loss and etc): Equal to or better than cases with conventional security methods

NOTE - Each of the above KPIs is application-dependent and is listed only as a reference value to be assumed. Each performance requirement will need to be refined in the future for each application.

Industry management (Remote robot operation)

This reference case outlines the capabilities of a maintenance expert who can remotely control on-site robots to carry out essential procedures. These procedures include thorough inspections, parts replacement, and valve closure as if the expert was physically present at the plant site.

The advanced remote maintenance capabilities enabled by this use case bring numerous benefits to the plant industry. It allows maintenance experts to make the most efficient use of their resources. It also enables long-term plant operations to be carried out in a safer, quicker, and cost-effective manner. Furthermore, the highly interactive communication applications developed for this use case have a wide range of potential applications beyond the plant industry, including healthcare, education, and entertainment. Leveraging these applications can further accelerate and improve businesses in these fields. [IOWN GF RIM RCRI]

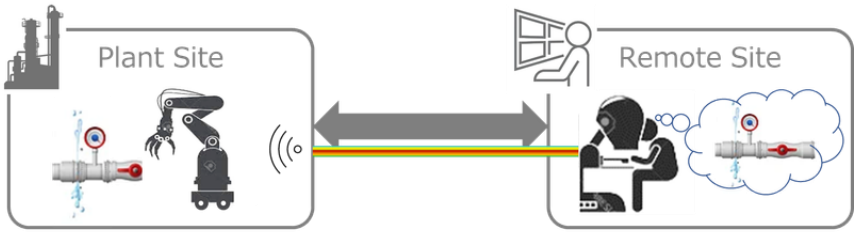

Figure 2-1: Overview of "Remote Controlled Robot Inspection" [IOWN GF RIM RCRI]

- Key performance requirements [IOWN GF RIM RCRI]
  - Manipulator control commands (Control input)
    - Latency: 100 ms
  - Manipulator feedback, including haptics information (Tactile feedback)
    - Latency: 10 ms
  - Video for operation (Video stream)
    - Latency: 100 ms
    - Bandwidth: 72Gbps (uncompressed), 2.5G bps (JPEG XS)

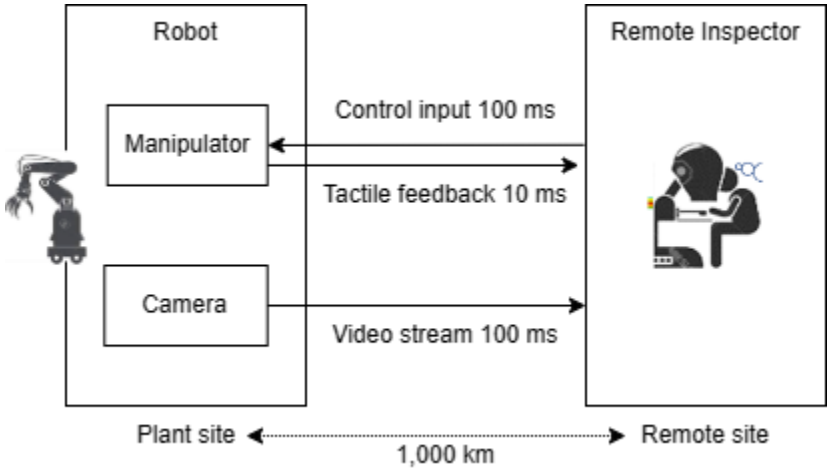

Figure 2-2: Latency diagram in RCRI [IOWN GF RIM RCRI]

3. Features and Requirements

This section describes desired features and requirements that the PoC of IOWNsec should satisfy.

Desired features of this PoC are

- PoC system is designed to combine multiple quantum-safe key exchange methods,
- PoC system has a key combining method to derivate shared keys for encryption, and
- PoC system interface has following sub-interfaces that the MFS system should provide for the business logic at a minimum (See the figure below for the location of Interfaces).
  - Communication interface
    - This is an interface for accepting data for cryptographic communication from the business logic to the MFS system. When this interface is called, key exchange methods are performed, the encryption key is combined from the multiple keys obtained, and encryption is performed by the encryption application inside the MFS system.
  - Setting interface
    - This is an administrative interface for configuration for key exchange combinations, key combining methods, encryption methods, etc. from business logic.

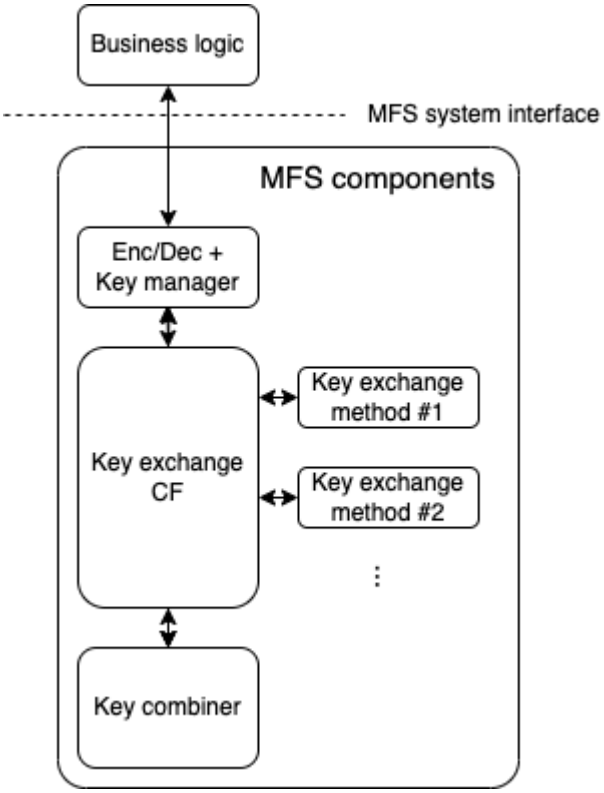

Figure 3-1: Location of the MFS system interface

Note 1: The “business logic” in the above figure includes not only applications that use cryptographic communications, but also applications for administrators.

Note 2: “Key exchange CF” in the above figure means Key exchange control function.

Note 3: The locations of the function blocks are examples and have no implementation restrictions.

Security requirements of this PoC are

- the key combining method must follow [NIST SP 800-133 Rev.2] and
- the cryptographic algorithm used as key exchange methods, authentication methods and encryption methods must have at least 128-bit security against quantum computers.

The above requirements are listed as minimums that MFS components must satisfy to achieve post-quantum security. The first requirement is that the method of generating cryptographic keys is critical to maintaining security, so the NIST recommendation regarding it should be followed. Regarding the second one, AES-256 is commonly considered to have post-quantum security. According to Grover's algorithm, AES-256 has 128-bit security against quantum computers. Therefore, the security requirement for the algorithm used in this PoC is set to have 128-bit security or higher against quantum computers. Specific cryptographic algorithms and physical security requirements are not specified in this PoC.

Performance requirements of this PoC based on reference cases are

- latency of cryptographic communication to be reached is recommended to be less than 10 ms and
- bandwidth of cryptographic communication must be at least 2.5 Gbps.

The above requirements ware determined with reference to the communication service requirements for remote robot operation described in Section 2. The scope of this PoC is to clarify the communication impact of MFS on conventional methods. Therefore, to create a PoC system that can evaluate this point with as little effort as possible, lower performance requirements ware set as a minimum line.

Regarding NW distance and bandwidth, it is recommended that multiple variations of them are evaluated in performance reports.

Implementers do not necessarily need to build a PoC system that includes all of the above features and may report based on a partial implementation of the MFS, however, they must implement all of the above desired features and requirements if implementers choose to "Milestone" as the PoC stage.

4. Subjects of Report and Key Benchmarks

This section identifies subjects and benchmarks that PoC implementers are expected to report.

4.1. Where MFS is Implemented

Implementers of this PoC are expected to report where MFS is implemented such as

- applicable location,
- applicable layer, and
- applicable protocol.

4.2. Implementation Architecture of MFS

The expected implementation architecture report points are

- shared key derivation,
- shared key synchronization, and
- updating key (rekey) for encryption, including shared key pooling.

4.3. Impact of MFS on Network Service Quality

The impact on network service quality when MFS is implemented needs to be demonstrated compared to the case without encryption or with conventional key exchange methods. In this PoC, the components consist of the MFS are broken down and the KPIs to evaluate are set so that the performance of the MFS can be verified even partially. MFS architecture is divided into three major components as shown in Figure 4.3-1.

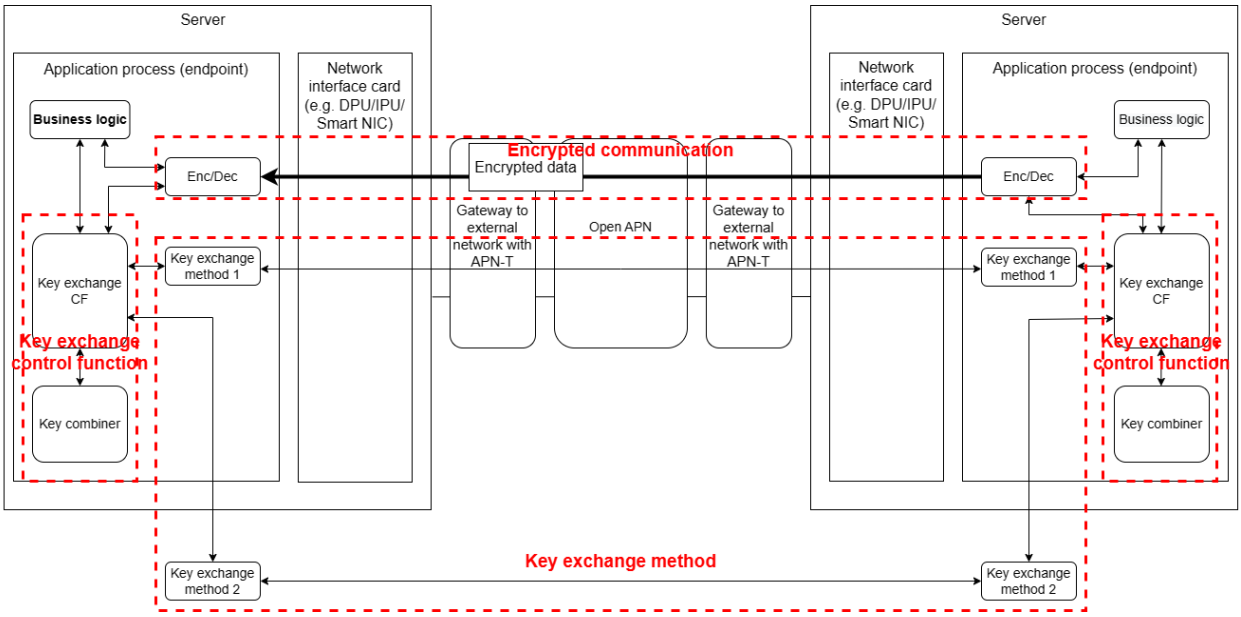

Figure 4.3-1: Segmentation of MFS architecture

4.3.1. KPIs to evaluate

KPIs related to key exchange and KPIs related to cryptographic communication are set separately. Only partial functions that consist of each KPI may be reported. A simple performance model to clarify each KPI is illustrated in Figure 4-3.2.

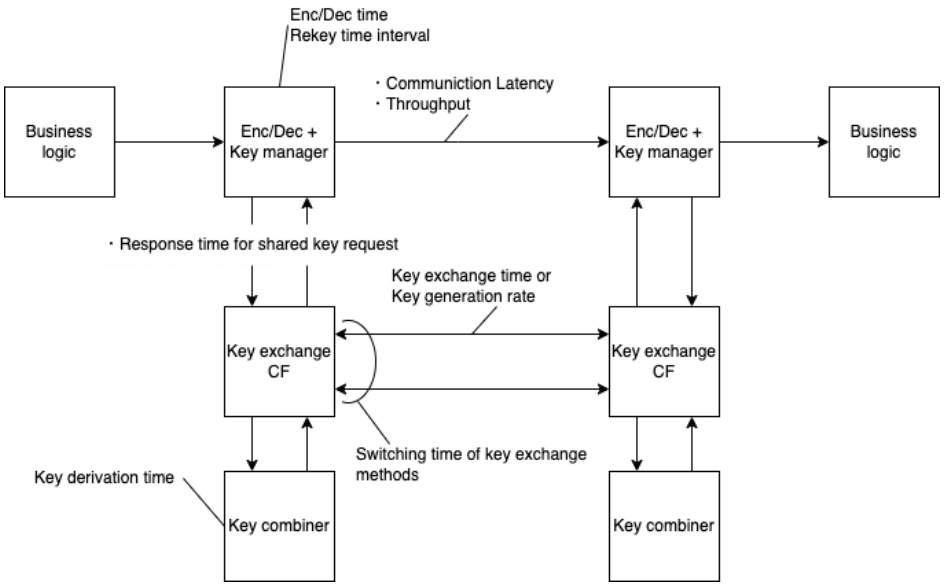

Figure 4.3-2: Simple performance model of MFS system

KPIs for key exchange method and key exchange control function (key exchange CF)

- Response time for shared key request
  - Key exchange time or Key generation rate of each key exchange method including authentication
  - Key derivation time
- Minimum rekey time interval: Minimum time interval for updating keys to limit the amount of data encrypted with the same key.
- Switching time of key exchange methods: Response time for a request to change a key exchange method combination.

NOTE - Technical information of key generation through the APN for QKD-based key exchange is included in Appendix C.

KPIs for encrypted communication

- Communication latency between IOWNsec endpoints or near-endpoints (Expected to be observed as a function of rekey interval.)
- Latency differences between encrypted communication with MFS and the following
  - Unencrypted communication
  - Encrypted communication utilizing existing key exchange methods (e.g., Elliptic Curve Diffie–Hellman) or encryption methods (e.g., existing encryption protocol with AES)
- Throughput of encrypted communication (Expected to be observed as a function of rekey interval.)
- Throughput differences between MFS and the following

  - Unencrypted communication
  - Encrypted communication utilizing existing key exchange methods (e.g., Elliptic Curve Diffie-Hellman) or encryption methods (e.g., existing encryption protocol with AES)
- Jitter (variation of latency) of encrypted communication: E.g., jitter per unit time when rekey is performed at regular intervals in stream communication. (Expected to be observed as a function of rekey interval.)
- Jitter differences between MFS and the following
  - Unencrypted communication
  - Encrypted communication utilizing existing key exchange methods (e.g., Elliptic Curve Diffie–Hellman) or encryption methods (e.g., existing encryption protocol with AES)
- Packet loss of encrypted communication
- Packet loss differences between MFS and the following
  - Unencrypted communication
  - Encrypted communication utilizing existing key exchange methods (e.g., Elliptic Curve Diffie–Hellman) or encryption methods (e.g., existing encryption protocol with AES)

NOTE - It would also be beneficial to measure differences in the above KPIs depending on the cryptographic algorithm or protocol used.

4.4. Power Consumption

The impact of the MFS on energy efficiency, one of the main KPIs identified by the IOWNGF, should be demonstrate. The adoption of MFS will inevitably increase power consumption due to the increased amount of computation compared to the unencrypted or conventional key exchange method, but the incremental power consumption should be clarified.

4.4.1. KPIs to evaluate

The metric for this benchmark should be selected based on the nature of communication. PoC implementers are free to choose a measuring methodology based on the nature of the communication they are assuming (e.g., whether it is streamed or discrete communication).

4.5. Applicability of IOWNsec Implementation

Since MFS is more complex than the conventional key exchange function, the ease of implementation of MFS also needs to be evaluated.

4.5.1. KPIs to evaluate

A report on the IFs of each component that consists of the MFS of the developed PoC system is expected.

5. Summary

The purpose of this PoC is to clarify the impact of MFS on the performance of data communication. First in this document, the context of this PoC Reference, purpose, objective and scope are introduced in Section 1. Following, use cases in which this PoC technology is assumed to be used are described in Section 2, along with reference performance values. Then, desired features and requirements of this PoC are given in Section 3, and finally, expected subjects of report and benchmarks to evaluate implementations of such features are detailed in Section 4.

IOWN GF is looking forward to receiving PoC Reports. The experiences in these reports will be reviewed and used to improve and guide the development of the IOWN GF Security specifications.

References

[IOWN GF RIM RCRI]: IOWN Global Forum, “Reference Implementation Model (RIM) for the Remote Controlled Robotic Inspection Use Case” 2023, https://iowngf.org/technology/

[IOWN GF SEC OUTLOOK]: IOWN Global Forum, “Technology Outlook of Information Security” 2022,

https://iowngf.org/technology/

[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

Appendix A: Examples of MFS applications

Example1: Implementation to optical transponder

Applicable location: Optical transponder

Applicable layer: Layer1 or 2

Applicable protocol: OTNsec or MACsec

Example2: Implementation to Smart NIC

Applicable location: Smart NIC

Applicable layer: Layer1 or 2

Applicable protocol: OTNsec or MACsec

Example3: Implementation to xPU with confidential computing

Applicable location: xPU

Applicable layer: Layer3 or higher

Applicable protocol: IPsec, TLS or contents encryption

Appendix B: Applicability of QKD-based Key Exchange

As described in “Technology Outlook of Information Security Version 1” document, QKD-based key exchange method are not performed by the application processes (endpoints) like PQC-based key exchange, but performed by the trusted third party’s infrastructure. Furthermore, it is assumed in the version 1 document that the QKD-based key exchange infrastructure is deemed independent of Open APN services, which means separate optical fiber infrastructure need to exist to carry “single photon” signals between neighboring QKD nodes for calculating the key.

History

Revision	Release Date	Summary of Changes
1	October 2023	Initial Release