大和総研
Daiwa Institute of Research

White Paper Summary: Proof of Concept Results for Post-Quantum Cryptography (PQC) in Online Services

July 24, 2026
Origin Publication Date (Japanese): March 31, 2026

Daiwa Institute of Research Ltd.

Disclaimer

This document summarizes current information on Post-Quantum Cryptography (PQC) and the results of verifications conducted within our group. The content is subject to change depending on future standardization trends, product implementation status, and changes in the threat environment.

The information provided in this document is for informational purposes only. Product names, company names, and service names mentioned herein are included for the purpose of explaining the demonstration environment, and do not constitute a guarantee or recommendation by our company for the adoption, performance, or future compatibility of any specific product or service.

The technical trends and product compatibility status described in this document are generally based on information as of March 2026.

Unless otherwise noted, all figures and tables in this document were created by Daiwa Institute of Research Ltd.

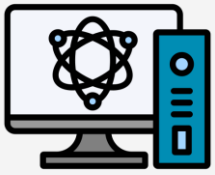
Table of Contents

1. Purpose and Background of the PQC Proof of Concept

- With the advancement of quantum computers, there are concerns about the declining security of conventional public-key cryptography, such as RSA and elliptic curve cryptography.
- The risk of "Harvest Now, Decrypt Later," where encrypted data is collected today to be decrypted by future quantum computers, could have a severe impact on customer and transaction information handled by financial institutions.
- In the United States, a roadmap has been outlined targeting the completion of the transition to PQC for national security systems by 2030.
- In Japan as well, discussions on the transition to PQC are underway, led by the Cabinet Secretariat and the National Center Office (NCO).
- Against this background, the Daiwa Securities Group conducted a proof of concept (PoC) to verify the technical and operational feasibility of Post-Quantum Cryptography (PQC) for its online services.

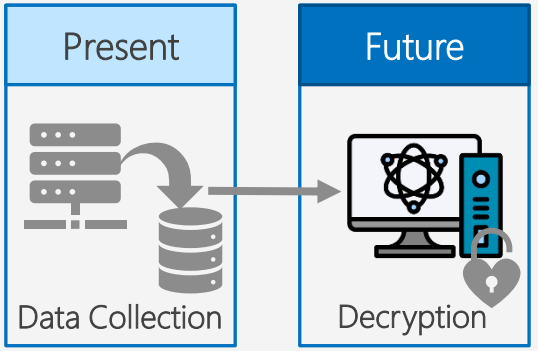
Compromise of conventional cryptography due to the emergence of quantum computers

- Public-key cryptography widely used on the Internet will be efficiently decrypted by quantum computers (Shor's algorithm).



Threat of "Harvest Now, Decrypt Later"

- The threat of collecting encrypted data and decrypting it after the emergence of quantum computers.



Focus on PQC in the financial sector

- In May 2025, the Financial Services Agency (FSA) requested banks and other institutions to begin addressing PQC.
- Discussions on PQC compliance are taking place, primarily among the Bank of Japan and mega-banks.

2. Overview and Structure of the Proof of Concept

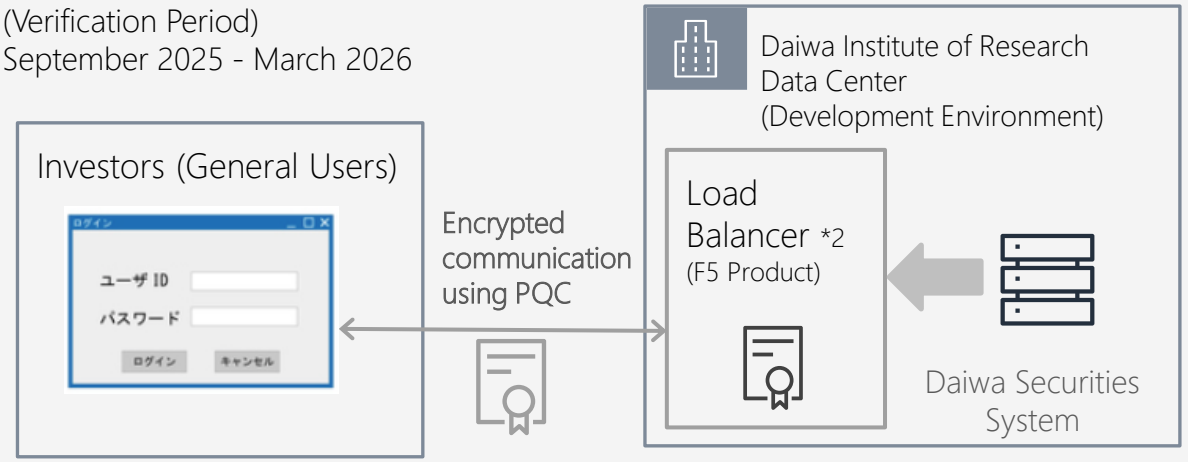
- The PoC was conducted using the development environment of Daiwa Securities' business systems.
- A joint verification by six companies: Daiwa Securities Group Inc., Daiwa Securities, Daiwa Institute of Research, NEC Corporation, F5 Networks Japan G.K., and DigiCert Japan G.K.
- The verification was conducted from September 2025 to March 2026, followed by the drafting of the white paper.

Overview of Verification

Verification of the impact of adopting PQC for encryption methods in Internet communications.

(Verification Method)
1. Introduced a load balancer compatible with PQC encryption methods.
2. Conducted load testing in the securities business system (development environment). Verified server load, performance, stability, etc.

(Verification Period)
September 2025 - March 2026



*2: Load balancer. Distributes processing load and performs encryption for Internet connections.

Roles of Each Company

Company	Role
Daiwa Securities Group Inc. / Daiwa Securities	• Formulation of PQC introduction policy • Consideration of application to online services • Formation of verification projects • Overall planning support from a user's perspective
Daiwa Institute of Research	• Preparation of verification environment • Creation of verification scenarios • Execution of verification and evaluation • Drafting of the white paper
NEC Corporation	• Scenario review, white paper review • Inclusion of the company's perspective
F5 Networks	• Provision of load balancer • Provision of PQC-compatible firmware.
DigiCert	• Provision of information on standardization trends for PQC and its digital signatures

3. Findings from the Proof of Concept (Summary)

- In this PoC, the technical impact (processing and communication) of the transition to PQC was evaluated. The results showed that the increase in processing time for PQC Key Encapsulation Mechanism (KEM) is minimal, and the impact on communication in the tested Daiwa Securities system was negligible, indicating no adverse effects on the transition or actual operations.
- However, as some technologies, such as digital signatures and authentication, are still undergoing standardization, it is necessary to formulate a transition plan that takes system replacement schedules into account.
- If necessary, a cryptography transition team should be formed to consider promoting a planned transition across the entire Daiwa Securities Group.

1. PoC Results

Transition to PQC for key exchange has no impact on the Daiwa Securities system

■ Key Encapsulation Mechanism (KEM)
The increase in processing time related to cryptography is negligible.
No impact on the Daiwa Securities system.

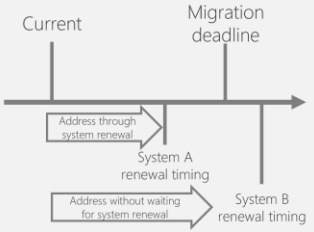
■ Digital Signatures (DSA)
Not yet standardized, making system-level evaluation difficult.
Since the impact of increased key size was confirmed in basic verification similar to KEM, the impact of increased signature size and its effect on communication should also be verified for DSA.

2. Standardization Trends

Need to assess standardization trends and system replacement timing

For areas not yet standardized, such as signatures and authentication, it is necessary to wait for standardization.

It is necessary to check standardization trends and transition deadline guidance to determine whether to align with system replacement timing or transition before replacement.



3. How to Proceed with the PQC Transition

Formation of a cryptography transition team and promotion of cryptography inventory creation

Although the PoC was conducted on a single system, it was found that there are multiple aspects to consider, such as the use of cryptography in various places other than TLS even within a single system, and the differing standardization status for each area.

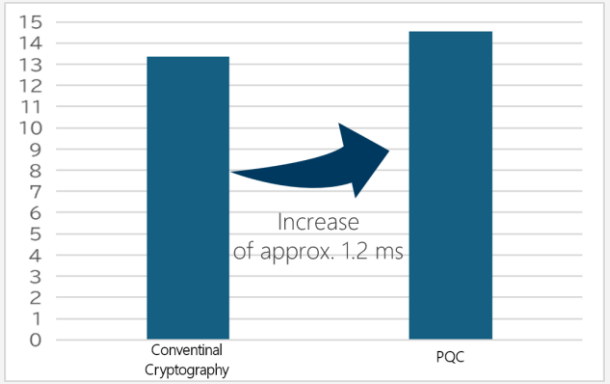
It is necessary to take a comprehensive view of the entire system and organize a cryptography inventory. A cross-group team for cryptography transition should be formed to investigate systems, create a cryptography inventory, and prepare for the transition.

(1) PoC Results

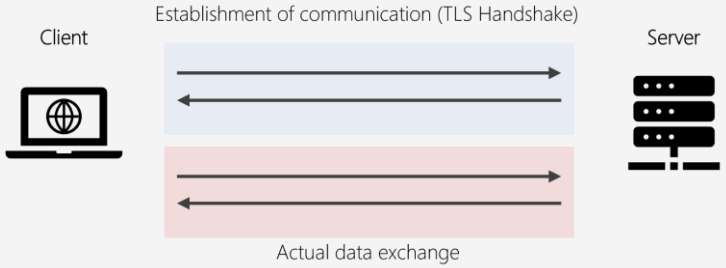
- As a result of the PoC, it was confirmed that in Internet encrypted communication, key exchange using PQC (ML-KEM) results in an extremely short increase in cryptographic calculation time, and the impact on the overall processing performance of establishing communication (TLS handshake) is negligible.
- On the other hand, the large key size of PQC increases the communication volume for both clients and servers, leading to an increase in the number of packets. Therefore, in environments with limited wireless communication or line bandwidth, communication impacts may occur, requiring prior evaluation before introduction. It was determined that there is no impact on the Daiwa Securities system, where sufficient line bandwidth is secured.

Comparison of processing time between conventional cryptography and PQC

- Comparing the time to establish communication using conventional cryptography and PQC, it was found that the communication time increased by an average of about 1.2 milliseconds.
- Compared to the processing time of the entire system, the increase is minimal and is considered to have almost no impact.



Increase in communication volume and number of packets due to increased key size



- PQC increases the communication volume for establishing communication. As a result, the number of packets also increases.

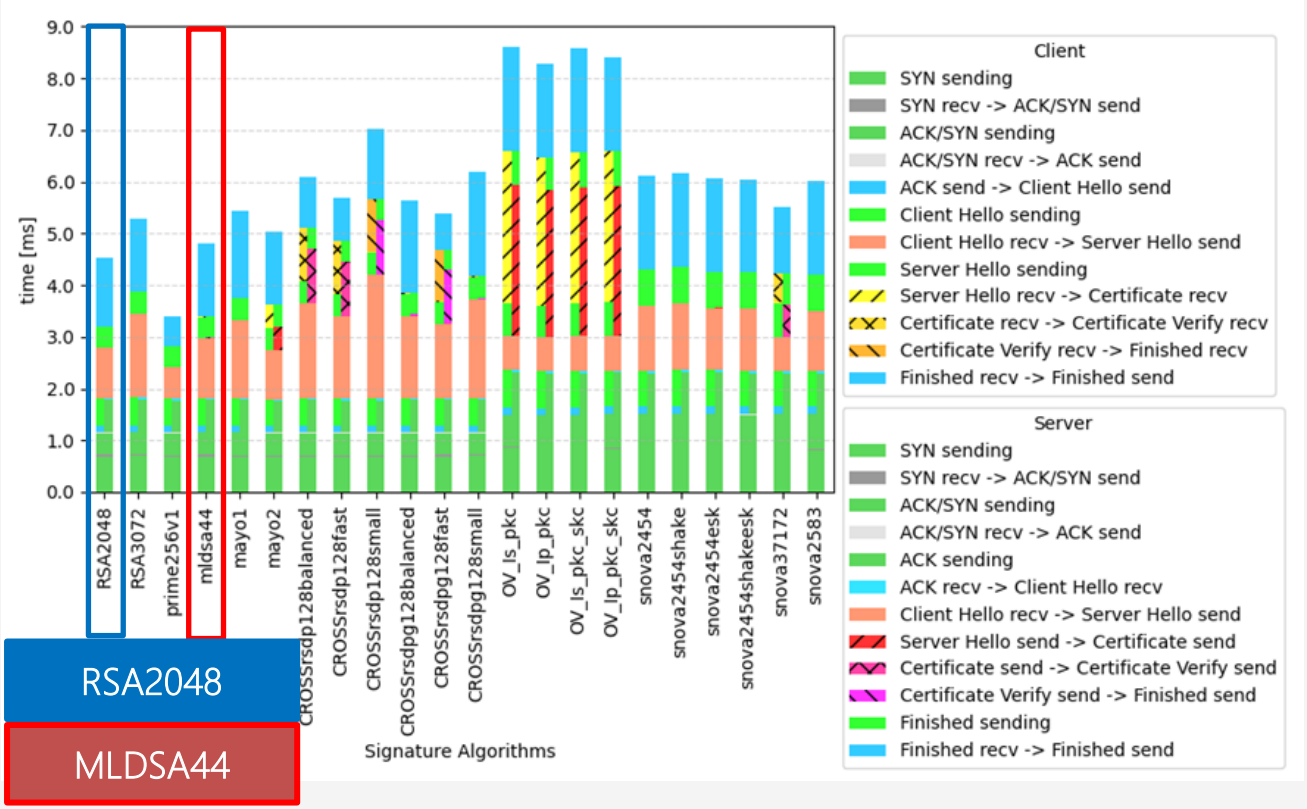
* Unit: Bytes

	Conventional Cryptography	PQC
Client	455	1631
Server	3661	4749
Packets	4	6

<Reference Information> Verification in AWS Environment Regarding Digital Signatures

- Regarding digital signatures, since the load balancer was not compatible, a PoC using the Daiwa Securities system could not be conducted. Therefore, basic verification was performed using a test machine in an AWS environment.
- As a result of the verification, it was found that for digital signatures, the ML-DSA algorithm selected by NIST **performs comparably to conventional cryptographic algorithms**.

Graph of communication speed by cryptography



- Compared to RSA2048 (2048-bit RSA cryptography), which is currently the mainstream RSA cryptography, the communication speed of ML-DSA, a PQC, is almost the same.

Note: NIST has selected multiple cryptographic algorithms for standardization as a contingency in case a selected algorithm is compromised. Accordingly, this verification also tested multiple algorithms.

(Environment Assumptions)

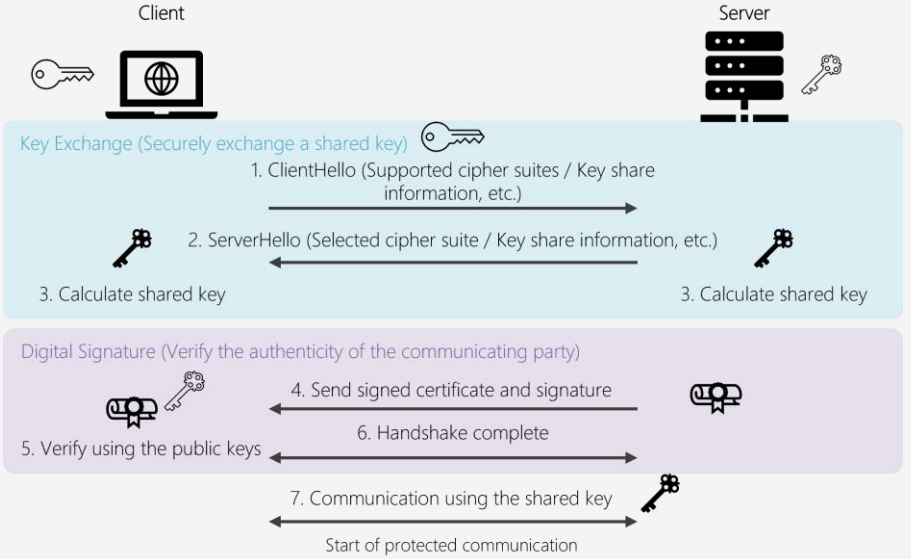
Key Exchange Algorithm: X25519

Root CA Signature Algorithm: P256

(2) Standardization Trends

- In TLS, which is Internet encrypted communication, public-key cryptography is used in two places: key exchange and digital signatures, and both need to be considered for the PQC transition.
- For key exchange, standardization by NIST (National Institute of Standards and Technology) has been completed, and the use of PQC is beginning.
- On the other hand, for digital signatures, standardization by the Internet Engineering Task Force (IETF) is incomplete, and support in hardware provided by various vendors has not yet progressed.
- Therefore, when transitioning TLS to PQC as of 2026, it is necessary to prioritize the standardized key exchange and address digital signatures in stages while closely monitoring standardization trends.
- For the Daiwa Securities Group systems as well, it is necessary to check standardization trends and transition deadline guidance to determine whether to align with system replacement timing or transition in advance.

TLS Communication Flow



Standardization completed by NIST / Social implementation has also begun

Standardization completed by NIST / Social implementation has not begun because standardization by IETF has not been conducted.

C. How to Proceed with the PQC Transition (1/2)

- Since the PQC transition is expected to be a long-term effort, establishing a cross-group structure (specialized team) is effective.
- Because cryptography transition will be required in many systems, **a dual-track approach can be considered, where highly important systems are managed separately from other systems based on system criticality**.
- While PQC assumes it cannot be efficiently breaking by quantum computers, there is a possibility that efficient attack methods may be discovered in the future. Therefore, the concept of crypto-agility—designing systems to easily transition to other cryptography—is also important.

Step 1: Structure Establishment

Establish a cross-group promotion team to formulate and drive the overall plan.

Step 2: Creation of Cryptography Inventory

Create a cryptography inventory detailing where and what cryptography is used.

Step 3: Risk Assessment and Prioritization

Evaluate systems to be transitioned based on impact, probability, transition difficulty, and confidentiality period.

Step 4: Roadmap Formulation

Create a transition roadmap using a dual-track approach that considers system criticality.

Step 5: Consideration of Transition Methods

Consider transition methods that ensure crypto-agility, taking future cryptographic changes into account.

Step 6: Impact Assessment

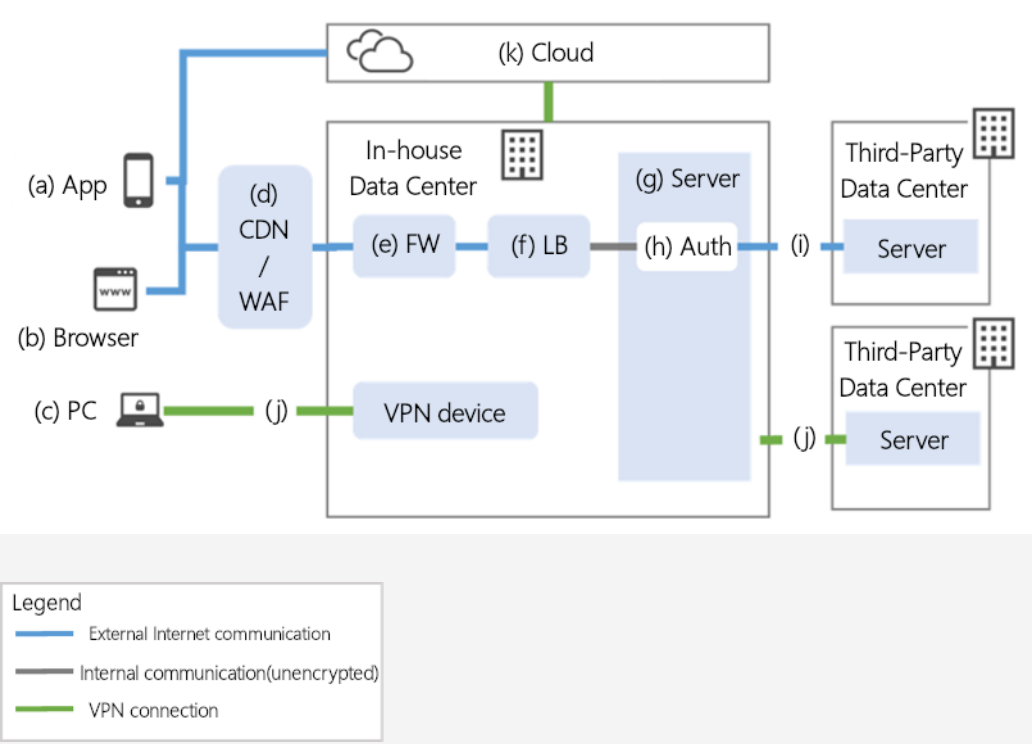
Recognize potential impacts before the transition, and confirm impacts and perform tuning after the transition.

(3) How to Proceed with the PQC Transition (2/2)

- When creating a cryptography inventory, a method of investigation using a system conceptual diagram like the one below can be considered.
- **Support is also required for authentication (Passkeys, SAML, OIDC, OAuth, etc.)** used in smartphone apps and server-side apps.

Note: Since standards are currently being formulated by organizations like IETF, it is necessary to check the status.

Cryptographic Usage Locations and Required Actions



Location	PQC Action Required
(a) App	If the smartphone app uses Passkeys, PQC migration is required.
(b) Browser	Major browsers are already compatible; generally no action required.
(c) PC	If PCs use VPN connections, PQC migration is required.
(d) CDN/WAF	The location requiring PQC action depends on where TLS is terminated (diagram assumes TLS termination at the load balancer).
(e) FW	
(f) LB	
(g) Server	
(h) Authentication	PQC migration required for SAML, OpenID Connect, OAuth, client authentication, etc.
(i) API Connection	PQC migration required for server-to-server API connections, in conjunction with (h).
(j) VPN Connection	PQC migration required where VPN connections exist.
(k) Cloud	Identify all TLS communication points within the cloud (CDN, FW, LB, etc.) and address accordingly. For managed services, action is pending the cloud vendor's service availability.