BIS Innovation Hub

Project Leap

Quantum-proofing payment systems

December 2025

BANCA D'ITALIA EUROSISTEMA

BANQUE DE FRANCE EUROSYSTÈME

DEUTSCHE BUNDESBANK EUROSYSTEM

nexi

Swift

www.bis.org

Executive summary

Protecting financial systems from the potential threat posed by quantum computers requires a proactive and coordinated approach. Challenges go beyond technical aspects and include awareness, resource allocation, competence development, inventory, pilots, governance and more.

Project Leap Phase 1 successfully tested the implementation of post-quantum cryptography between two central banks (BISIH et al (2023)). A traditional public key algorithm was implemented alongside quantum-resistant algorithms in a hybrid encryption scheme, achieving quantum-resistant confidentiality of payment messages sent between two distanced IT systems. The project demonstrated that implementing quantum-safe cryptography in the financial system is feasible and identified the need for more testing.

Project Leap Phase 2, a collaboration between the BIS Innovation Hub Eurosystem Centre, Bank of Italy, Bank of France, Deutsche Bundesbank, Nexi-Colt and Swift, tested post-quantum cryptography in an operational payment system. Most payment systems rely on public key cryptography and require long-term data confidentiality, making them vulnerable to the quantum computing threat. At the same time, as the backbone of modern economies, payment systems are critical to the smooth functioning of commerce, finance and daily life – protecting them is essential to preserving financial stability.

The experiment of Project Leap Phase 2 replaced traditional digital signatures with post-quantum cryptography when sending liquidity transfers in the Eurosystem's Target2 system. It involved functional, performance and interoperability testing. All test scenarios were successfully executed, demonstrating the feasibility of migrating payment systems to post-quantum cryptography. The tests also revealed significant performance differences between traditional and post-quantum algorithms, pointing at the need for further testing and preparation before transitioning the financial system.

The two successful technical experiments of Project Leap Phases 1 and 2 have laid important groundwork for the quantum-safe journey of payment systems, underscoring the commitment of central banks and private partners to proactively safeguarding the integrity and resilience of existing and future financial infrastructures. They reflect a forward-looking dedication to ensuring that payment systems remain secure in the face of emerging technological threats.

Acronyms, abbreviations and definitions

API	Application programming interface
A2A	Application to application
AES	Advanced Encryption Standard is a symmetric encryption algorithm widely used to secure data. It operates on fixed-size blocks (typically 128 bits) and uses key sizes of 128, 192 or 256 bits.
BAH	Business application header is a mandatory ISO 20022 header segment in T2 payment messages that contains business-level routing and identification details.
CRDM	Common reference data management is a component that centralises data reference management (eg user accounts, authorisations and configuration parameters) across all TARGET services, ensuring consistency and streamlined operations.
DEP	Data exchange protocol is a communication protocol standard of T2 serving at differentiating proprietary communication protocols used by different NSPs.
ECC	Elliptic curve cryptography is a public key cryptographic system based on the algebraic structure of elliptic curves over finite fields. It provides the same level of security as traditional methods like RSA but with much smaller key sizes, making it more efficient in terms of speed, storage and power consumption.
ESMIG	Eurosystem single market infrastructure gateway is a unified technical gateway that permits access to all TARGET services (like T2, T2-Securities (T2S), T2 Instant Payment System (TIPS) and Eurosystem Collateral Management System (ECMS)) through a single, secure interface.
FMIs	Financial market infrastructures
HSM	Hardware security module
ISO	International Organization for Standardization
NSP	Network service provider
IETF	Internet Engineering Task Force
NIST	National Institute of Standards and Technology
PQC	Post-quantum cryptography
RTGS	Real-time gross settlement systems process high-value payments in real time and in central bank money, ensuring safe and immediate settlement and supporting monetary policy and financial stability.
RSA	Rivest-Shamir-Adleman is a widely used public key cryptographic algorithm that enables secure data transmission. It relies on the mathematical properties of large prime numbers and modular arithmetic.

Table of contents

1. Introduction

The transition towards quantum-safe environments within the financial sector is urgent. Although the exact timeline for developing a cryptographically relevant quantum computer remains uncertain, its potential to compromise current public key cryptography poses an imminent threat to today's financial system (Auer et al (2025)).

The core threat of quantum computing lies in its potential to compromise many of today's widely used cryptographic algorithms, the backbone of modern secure communications. Quantum computers rely on unique quantum-mechanical properties for computation, and they are capable of solving the mathematical problems behind today's cryptographic algorithms. Shor's algorithm, when implemented on a quantum computer, can factor large integers in polynomial time, threatening widely used asymmetric cryptographic algorithms. Tasks which today require millennia of computation time on a classical computer could be achieved in under a week by a quantum computer with fewer than a million noisy qubits (Gidney (2025)). Although it is more resistant, symmetric cryptography is not immune either – Grover's algorithm executed on a quantum computer provides a quadratic speedup over classical methods, requiring longer keys to maintain the same level of security in the quantum era (Grassl et al (2015)).

Moreover, vulnerabilities particularly affect digital signatures and authentication protocols, which are critical to payment systems and financial market infrastructures (FMIs). Digital signatures, typically based on asymmetric cryptography, ensure data integrity, authenticate the identity of senders and prevent the alteration of transaction messages. Should quantum computers become sufficiently powerful, they could compromise these signatures and undermine trust in financial communication systems.

An important concern is the "harvest now, decrypt later" scenario whereby malicious actors may already capture and store encrypted data transmitted over the internet today with a view to decrypting them using future quantum computers. Given the longevity and sensitivity of financial data, this type of quantum threat demands immediate action. Data confidentiality must be secured for extensive periods – often decades – meaning any delay in transitioning to quantum-resistant cryptography effectively exposes current financial data and communications to future compromise. This underscores the urgency highlighted in Project Leap: central banks and FMIs must begin their migration to quantum-safe environments immediately to mitigate risks posed by the rapid and unpredictable evolution of quantum computing capabilities.

2. Defending payment systems against the quantum threat

2.1. Payment systems and financial market infrastructures

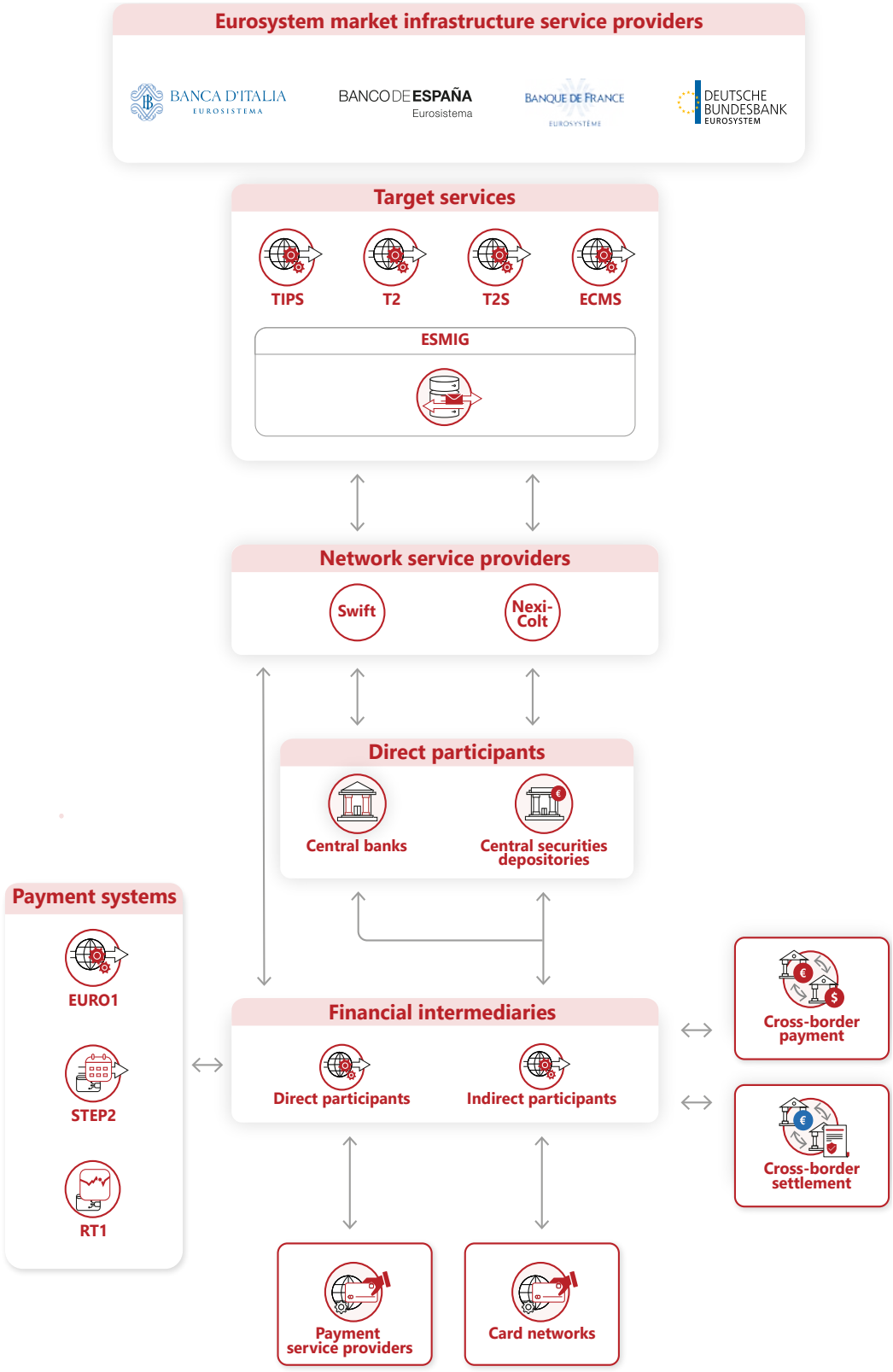
Global FMIs represent the backbone of the world's financial ecosystem and are vital to economic activity and growth. They collectively handle all high-value and retail transfers and ensure the smooth circulation of assets among banks, businesses and individuals. While each infrastructure has its own operational focus and jurisdictional scope, their collective functioning underpins the trust and efficiency of modern finance in the world.

Payment systems serve as a central component of a jurisdiction to ensure efficient and secure monetary transactions. Their ability to ensure irrevocable settlement fosters confidence among the general public, contributes to financial stability and reduces systemic risk. Among these systems, T2 is a critical infrastructure operated by the Eurosystem. It is designed to process real-time settlement of large-value payments in central bank money (see Graph 1).

Other prominent FMIs facilitate key functions across different regions and asset classes. Large-value payment systems such as Fedwire in the United States and CHAPS in the United Kingdom serve similar purposes in their respective currencies and are complemented by specialised services such as CLS[1] that mitigates settlement risk in foreign exchange transactions by synchronising payments across multiple currencies. Equally important are central counterparties including LCH[2] and Eurex[3] , which interpose between buyers and sellers to provide clearing services for derivatives and other financial instruments. Central securities depositories, such as Depository Trust Company in the United States and Euroclear in Europe, safeguard and manage the issuance, custody and settlement of a wide range of securities. Additionally, card networks power an enormous volume of consumer-level transactions globally. Specialised cross-border communication and settlement networks, accessed through network service providers (NSPs), enable banks to connect securely and exchange standardised payment and settlement instructions on a near real-time basis.

1. Continuous Linked Settlement (CLS) is a global payment system launched in 2002 to reduce settlement risk in foreign exchange transactions. It operates under the oversight of major central banks and currently supports 18 currencies, including the US dollar, euro, British pound, Japanese yen, Swiss franc and others from countries across North America, Europe, and Asia-Pacific. CLS settles both sides of an FX trade simultaneously through a centralised platform, ensuring that neither party is exposed to principal risk.
2. The London Clearing House (LCH), established in 1888 in the UK, is a central counterparty that clears and settles trades in derivatives, securities and other financial instruments.
3. Eurex, founded in 1998, is a European derivatives exchange that provides trading and clearing services through Eurex Clearing for futures, options and other derivatives across equities, interest rates, and indices.

The landscape of Eurosystem FMIs Graph 1



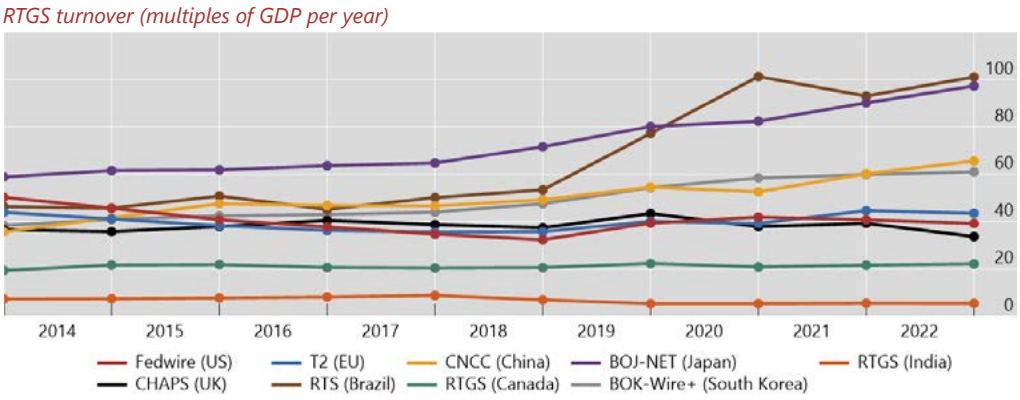
At the core of modern FMIs lie stringent cryptographic protocols designed to ensure data confidentiality, integrity and authentication, as well as non-repudiation. Many large-value payment systems, such as real-time gross settlement (RTGS) system arrangements, generally adhere to recognised standards put forward by national or international bodies including the Internet Engineering Task Force (IETF), National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO). According to such guidance, participant authentication and initial key exchange often leverage asymmetric cryptographic algorithms (eg Rivest-Shamir-Adleman (RSA) or elliptic curve cryptography (ECC)). Subsequently, these systems switch to symmetric algorithms such as Advanced Encryption Standard (AES) for bulk data encryption – an approach that balances robust authentication with the high throughput needed to handle large payment messages in near real time. In a typical high-value payment workflow, transactions originate from financial institutions and then pass through secure gateways before final settlement is recorded by a central bank. At each stage, cryptographic controls confirm the legitimacy of the transaction – digital signatures bind the sender's identity, hashing functions verify that data have not been altered and message authentication codes provide additional measures to detect any tampering in transit.

Card networks employ a similar dual approach to cryptography – public key algorithms for offline authentication (for example, chip and PIN terminals), combined with symmetric encryption for online authorisations. Communication between banks, payment processors and payment gateways relies on protocols like Transport Layer Security to protect data in transit. Cross-border transactions, especially those involving international financial messaging, follow widely accepted guidelines by using layered encryption and mutual authentication. Most of the cryptographic protocols currently used are vulnerable to a quantum computer attack.

2.2. The quantum threat

The strategic importance of quantum-proofing the financial system stems from the latter's foundational role in ensuring market stability and public confidence. Should these systems be rendered vulnerable by future quantum attacks, the ramifications could be rapid and systemic, far exceeding localised cyber incidents.

Annual RTGS value compared to GDP — Graph 2



At the wholesale level, the backbone of the global financial system rests on RTGS infrastructure such as Fedwire (United States), T2 (Europe), CHAPS (United Kingdom) or BOJ-NET (Japan). These systems settle transactions worth many multiples of GDP per year, enabling interbank lending, securities settlement and monetary policy operations (see Graph 2). Their criticality means that any disruption could have far-reaching consequences. The Hudson Institute has estimated that a quantum enabled cyber attack on Fedwire alone could decrease US real GDP by between 10 and 17%, causing between USD 2 and USD 3.3 trillion in indirect losses as measured by GDP at risk (Butler and Herman (2023)). This illustrates how wholesale settlement is not just "plumbing" for the financial sector, but the foundation upon which credit, liquidity and economic activity rest.

Further, simulations by Eisenbach et al (2020) show that impairing even one of the largest payment system participants can induce widespread liquidity blockages, potentially forcing central banks or other authorities to step in to maintain market functioning.

Quantum vulnerabilities cut across domestic and international finance, highlighting the reliance of market participants on globally recognised encryption standards. Cross-border trade, foreign exchange transactions and international capital flows all depend on secure messaging networks that quantum adversaries could eventually compromise. In this environment, even short-lived uncertainty about the reliability of cryptographic safeguards might trigger a sudden withdrawal of liquidity from markets perceived as at-risk. Compounded by the potential manipulation of settlement instructions or digital contract signatures, the fallout could affect everything from consumer payments to large-scale asset transactions.

2.3. Quantum-readiness initiatives

Central bank and financial sector initiatives

Responding to the quantum threat to current FMIs, central banks and financial institutions have begun to coordinate initiatives to transition towards quantum-safe cryptographic schemes for the banking sector. In 2023, in Project Leap Phase 1, a quantum-safe hybrid virtual private network was set up, demonstrating the feasibility of securing payment messages with post-quantum encryption schemes (BISIH et al (2023)). In July 2025, the Bank for International Settlements (BIS) published a paper detailing a quantum-readiness roadmap for the financial system, advocating immediate cryptographic inventories, cryptographic agility, defence-in-depth architectures, hybrid models and phased migrations to facilitate a systematic transition to quantum-resistant systems (Auer et al (2025)). The Monetary Authority of Singapore published guidelines for the financial system in 2024. It recommended that all financial institutions maintain exhaustive cryptographic asset inventories, prioritise systems for post-quantum cryptography (PQC) migration, and develop cryptographic agility strategies and capabilities to mitigate quantum threats (MAS (2024)). In the same year, the Bank of France and MAS conducted a cross-continental PQC experiment securing email communications with PQC algorithms (Bank of France (2024)).

In 2024, Europol launched the Quantum Safe Financial Forum to convene central banks, financial institutions and law enforcement stakeholders. This is a multi-stakeholder effort to address the transition to quantum-safe solutions across the financial sector. The forum is engaged in initiatives to prevent fragmented responses to quantum threats and

to develop cryptographic agility across the financial system. In 2025, Europol published a call to action promoting a coordinated roadmap and best practice sharing to accelerate the transition to PQC, securing the global financial ecosystem (Europol (2025)).

The Bank of Canada has published research on privacy-preserving post-quantum credentials for digital payments (Kazmi et al (2023)), and the Bank of Italy has issued studies on quantum-safe payment systems with quantum random number generation and quantum key distribution, [4] as well as broader strategies for secure financial systems (Bucciol & Tiberi (2023); Andriani et al (2024)). The Central Bank of Brazil has tested PQC methods applied to its instant payment system Pix (Ferreira et al (2022)).

Private sector initiatives are also emerging. Visa and JPMorgan Chase have been preparing for quantum risks (Castellanos (2020)), while HSBC and PayPal have jointly trialled quantum-safe cryptography for payments (Finextra (2024)), and Mastercard has developed precautionary frameworks against quantum cyber threats (Gibson (2024)).

At the multilateral coordination level, the G7 Cyber Expert Group's, co-chaired by the US Treasury and Bank of England, has urged financial authorities and institutions to develop a better understanding of quantum computing risks, assess vulnerabilities in their areas of responsibility, and establish governance processes and action plans for a safe PQC transition (G7 Cyber Expert Group (2024)).

Governmental initiatives

National regulators have reinforced the need for quantum-safe migration efforts through technical standards. In the United States, the Quantum Computing Cybersecurity Preparedness Act (Public Law 117-260, 21 December 2022) requires federal agencies to establish and maintain an inventory of "vulnerable" systems, prioritise assets for migration to post-quantum cryptography and submit migration planning reports to Congress within a specified deadline. Concurrently, the Cybersecurity and Infrastructure Security Agency's Post-quantum Cryptography Initiative, announced on 6 July 2022, established four pillars: (i) risk assessment across national critical functions; (ii) planning; (iii) policy and standards development; and (iv) stakeholders' engagement to drive a coordinated transition for both public and private sector infrastructure (CISA (2022)). Underpinning these efforts, NIST's ongoing PQC standardisation programme, initiated in 2016, delivered its standards in August 2024 (Jackson et al (2023); (NIST (2024b, 2025)).

In Europe, the Network and Information Security Directive 2, transposed into national law by October 2024, broadens mandatory cyber security requirements to "essential" and "important" entities (including FMIs), and requires EU member states to issue a roadmap and timeline to start using quantum-resistant forms of cyber security. This initiative reflects growing awareness of the risks posed by quantum computers. Building on this, the Network and Information Systems Cooperation Group's June 2025 roadmap urges member states to complete risk assessments and begin PQC migrations by 2026, targeting the full transition of critical systems by 2030 (NIS Cooperation Group (2025)). Meanwhile, the EU Quantum Europe Strategy, adopted in July 2025, allocates at least EUR 1 billion over ten years through the Quantum Technologies Flagship initiative and sets out five priority areas – research, infrastructures (including a pilot quantum internet), ecosystem

4. Quantum key distribution is a secure communication method that uses quantum mechanics to generate and share encryption keys, ensuring that any eavesdropping attempts can be detected.

strengthening, space and dual-use applications and quantum skills – to position Europe as a global leader by 2030 (European Commission (2025)). Canada's National Quantum Strategy focuses on meeting post-quantum requirements, transitioning IT systems to PQC and auditing compliance against evolving standards (ISED-ISDE (2023)).

Cyber security agencies across the globe have issued a series of recommendations to guide the transition towards hybrid quantum-safe cryptographic solutions. The European Telecommunications Standards Institute published a technical specification defining quantum-safe hybrid key establishment mechanisms, combining classical and post-quantum cryptographic algorithms. Hybridisation will ensure continuity and resilience during the transition phase. It is designed to leverage the maturity of traditional cryptography while introducing quantum-safe cryptography. The UK National Cyber Security Centre states in a white paper that "there is likely to be a period during which organisations will be required to operate both conventional and quantum-safe cryptography, in order to ease transition between the two" (NCSC (2020)). Similarly, a joint statement from 21 national European cyber agencies, including the French Cybersecurity Agency (ANSSI) and the German Federal Office for Information Security (BSI), recommends hybridisation as a pragmatic interim solution (BSI et al (2025)). This means combining a traditional cryptographic scheme in a way that helps ensure security even if one of its components is broken. While PQC is still maturing, hybrid approaches offer a balanced path forward by combining the proven robustness of traditional algorithms with the emerging security of PQC.

3. Project overview

3.1. Objective and scope

Project Leap Phase 2 aimed at implementing quantum-safe cryptography in the Eurosystem's payment system T2. It tested PQC signature schemes within T2 payment messages, focusing on selected system components. This involved integrating new cryptographic protocols into the message structure and ensuring their correctness, robustness and compliance with existing cryptographic standards.

An existing T2 test environment was selected to test quantum-safe cryptographic protocols. The test environment's configuration reflects realistic operational scenarios while ensuring a secure and isolated space for validating the integration of PQC mechanisms without impacting live operations. This setup allows for comprehensive end-to-end testing, including key generation, signature application and message verification under conditions aligned with production environments. The environment also supports different configurations and network topologies of the participating central banks, ensuring broad interoperability across varying infrastructures.

The tests focused on application to application (A2A) transactions for liquidity transfers. Among the various payment transactions processed daily in T2, liquidity transactions are the most commonly executed. This use case also reflects day-to-day operations in payment systems in other jurisdictions. It further presented the advantage of involving all project partners. To avoid unnecessary complexity, the scope of the project was limited to inbound communications only.

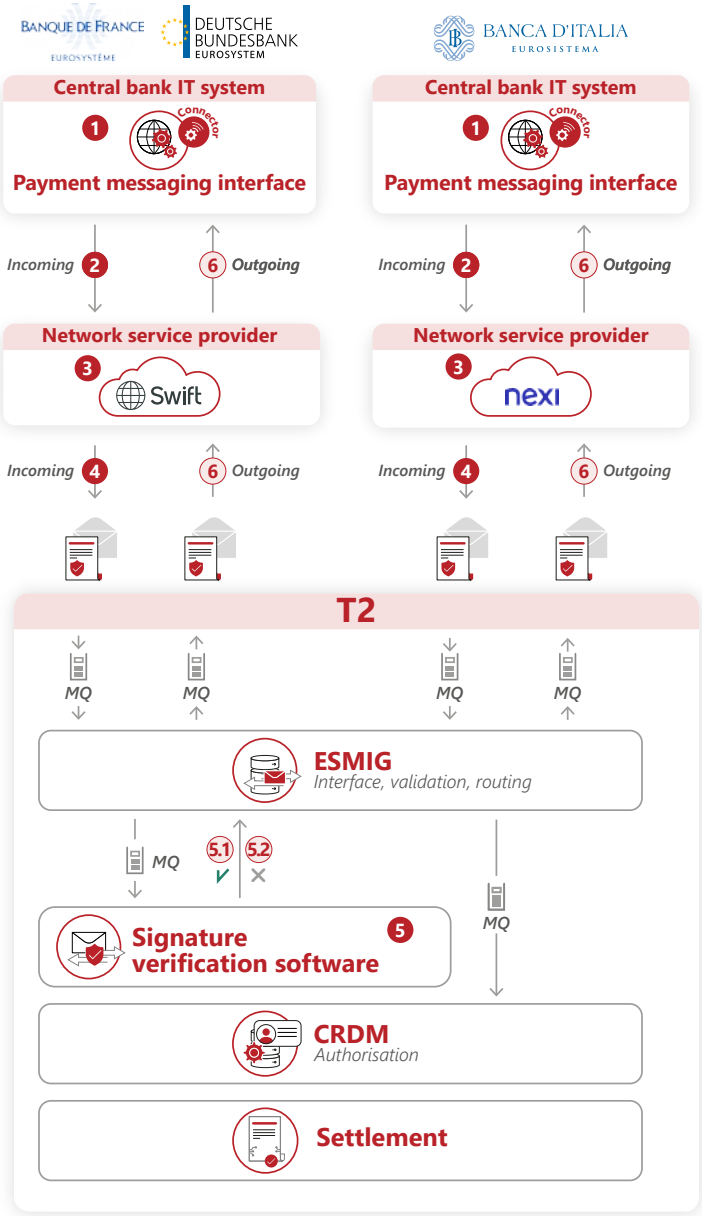
To deliver this project, the BIS Innovation Hub Eurosystem Centre and the participating central banks collaborated with Swift and Nexi-Colt. Bank of Italy, Deutsche Bundesbank and Bank of France experts operated in the capacity of payment systems and cryptographic protocols specialists. Swift and Nexi-Colt facilitated the connection to network solutions and delivered updated software to central bank teams for implementation. They also provided technical expertise during the configuration and testing phases.

The technical experiment required extensive planning, tight collaboration and commitment from different departments across organisations, including payment system experts, cryptography experts, and legal and procurement departments. The project illustrates that migration to quantum-safe cryptography is not a simple cryptographic protocol update, but a major transition that requires broad collaboration within and across organisations (Auer et al (2024, 2025)).

3.2. System description

Graph 3 shows the payment system infrastructure used for testing, as well as the payment flow from the client generating the payment message to the payment system accepting the transaction and sending back a response.

Payment system and transaction flow — Graph 3



1. *Client generates a payment message (camt.050 and head.001) without signature.*
   Client requests an authorised digital signature using a private key stored in an HSM.
   HSM generates encrypting signature and returns it to client.
   Client adds signature to head.001 and wraps the message within an NSP-protocol.
2. *Client sends the message to NSP.*
3. *NSP transforms the NSP protocol into DEP. NSP signs the message.*
4. *NSP forwards DEP-wrapped message to ESMIG.*
5. *Signature verification software verifies the signature.*

5.1 *If successful: ESMIG forwards the message to T2. The business matter is checked, as well as the certificate validity. If the payment message is received and processed, a message type camt.025 is sent with the receipt status report.*

5.2 *If not successful: ESMIG returns an admi.007 message type.*

6. *ESMIG-outbound component sends encrypted return message to client via the payment network.*

In T2, the entry point for A2A messaging is managed by Eurosystem single market infrastructure gateway (ESMIG). This gateway ensures secure reception, dispatch and routing of messages between users and other applications within T2. It serves as the central communication interface between the external world and internal T2 services. As shown in Graph 3, after the payment message format is validated by ESMIG, it is sent to the signature verification software,[5] which verifies the cryptographic aspects of the payment transaction. The signature verification software acts as a middleware layer fully integrated with ESMIG. It ensures compliance with security policies and cryptographic standards, often through configurable trust and validation rules. Once the digital signature is accepted, the message is sent back to ESMIG to be transmitted directly to the common reference data management (CRDM) module and ultimately to settlement.

The project focused on implementing and testing post-quantum digital signatures at the business application header (BAH) level of payment messages. The BAH, also known as head.001, is the standardised header used in ISO 20022 payment messages. It provides metadata about the message such as the message type (eg pacs.008, camt.053), the sender and receiver identification, creation date and time, and, most importantly for the technical experiment, the digital signature. The BAH was deliberately selected to ensure that the digital signature could be verified and validated early in the workflow, providing an efficient mechanism to authenticate the message's origin and integrity before it enters deeper stages of processing. For the purpose of the technical experiment, the BAH digital signature, which uses RSA in today's system, was replaced by a post-quantum signature using CRYSTALS-Dilithium [6] with a NIST security strength category 3.[7]

While sending payment messages, the generation and verification of the new post-quantum digital signature were assessed. The initial step in the experiment involved generating a post-quantum digital signature and subsequently assessing the system's ability to validate it, using an updated verification mechanism. Furthermore, the system's cryptographic agility was assessed, including the possibility of hybrid signature implementation. The experiment also included testing the system's capability to reject messages signed with invalid signatures. Ultimately, interoperability between systems was a prerequisite for the success of the project. These tests served as a foundational check to determine compatibility between the new cryptographic primitives and the current infrastructure.

5. The signature verification software is designed to perform cryptographic operations, such as digital signature verification. It leverages underlying cryptographic libraries and hardware security features. It allows cryptographic validation to be executed in a controlled, auditable and hardware-accelerated environment, playing a critical role in maintaining data integrity and trust, ensuring that only messages signed with valid digital signatures are accepted.
6. CRYSTALS-Dilithium (IV), NIST Round 3 (OID 1.3.6.1.4.1.2.267.7.6.5) (see Ducas et al (2021))
7. Due to technical limitations and the dedicated time frame, it was not possible to test the more recent version of the algorithm which is named ML-DSA. This aspect will need to be addressed in future testing phases as this latest version is the standardised one.

3.3. Test configuration and limitations

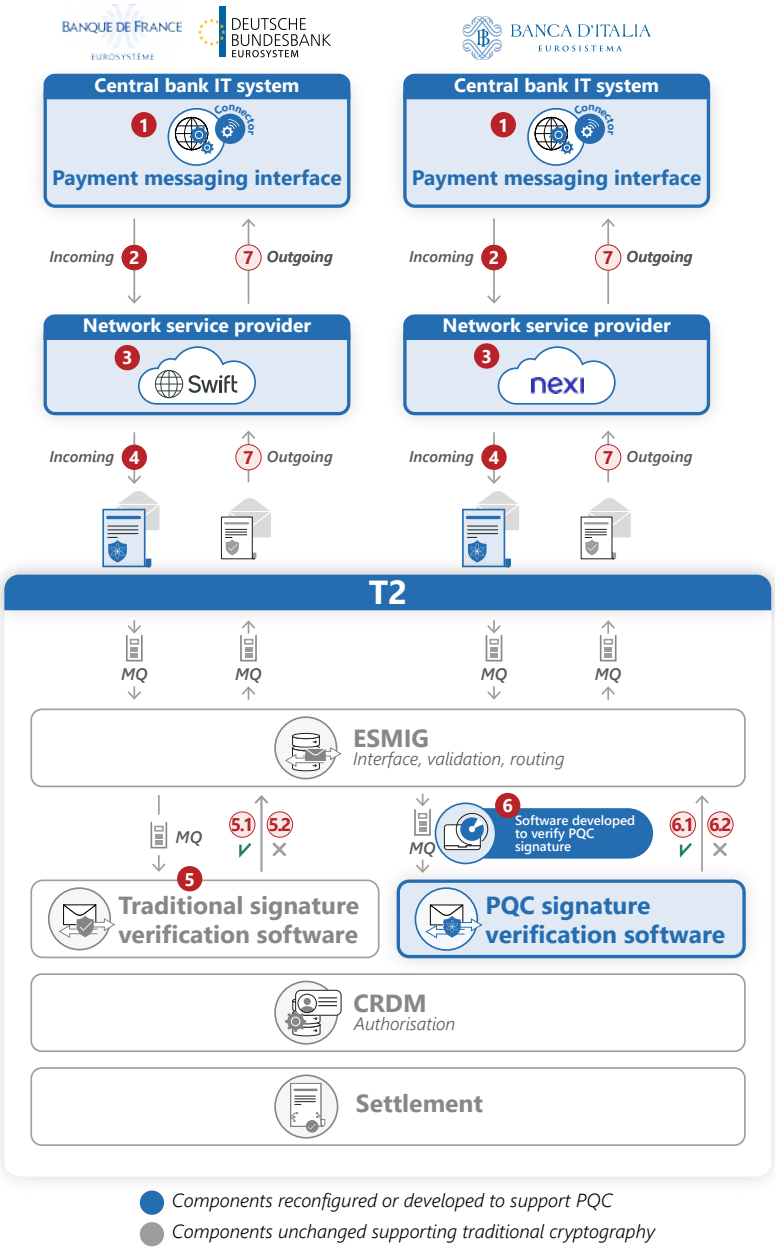
The Leap technical experiment involved modifying numerous system components. All participants were required to either reconfigure existing software or develop new components to ensure compatibility with the updated cryptographic libraries (Graph 4 highlights updated components in blue). Testing the exchange of payment messages relies on dedicated communications infrastructure utilised by multiple actors. Each central bank IT system utilises a specific communications infrastructure, reflecting varied national configurations (see Annex).

Central banks installed a PQC-enabled version of the software internally, allowing their connection to NSPs. The two participating NSPs consistently updated their network software and contributed with the provision of an updated version of their modules that included post-quantum cryptographic keys and testing sets. Additionally, NSPs provided central banks with a modified ESMIG connector to support PQC signatures at the BAH level. T2 participants reconfigured the ESMIG connector and the signature verification software in partnership with a solution vendor.

For the purpose of the PQC integration and testing activities, the use of a physical hardware security module (HSM) was temporarily replaced by a software-based key file approach. This substitution provided the flexibility required for rapid configuration changes and easier management of cryptographic material during the testing phase, while still supporting the core cryptographic functions necessary for validation. As part of the setup, central banks configured post-quantum cryptographic keys to validate both successful and failure test scenarios.

Test environment configurations

Graph 4



Components reconfigured or developed to support PQC

Components unchanged supporting traditional cryptography

1. *Client generates a payment message (camt.050 and head.001) without signature.*
   Client requests an authorised digital signature using a private key.
   Encrypting signature is generated and returned it to client.
   Client adds signature to head.001 and wraps the message within an NSP protocol.
2. *Client sends the message to NSP.*
3. *NSP transforms the NSP protocol into DEP. NSP signs the message.*
4. *NSP forwards DEP-wrapped message to ESMIG.*
5. *Signature verification software verifies the signature.*
- 5.1 *If successful: ESMIG forwards the message to T2. The business matter is checked, as well as the certificate validity. If the payment message is received and processed, a message type camt.025 is sent with the receipt status report.*
- 5.2 *If not successful: ESMIG returns an admi.007 message type.*
6. *Signature verification software verifies the PQC signature.*
- 6.1 *If successful: ESMIG forwards the message to T2. The business matter is checked, as well as the certificate validity.*
  If the payment message is received and processed, a message type camt.025 is sent with the receipt status report.
- 6.2 *If not successful: ESMIG returns an admi.007 message type.*
7. *ESMIG-outbound component sends encrypted return message to client via the payment network.*

One limitation was related to hybrid cryptographic implementation, where both PQC and traditional signatures would need to be processed in parallel. The existing structure of the signature verification software configuration only accepts one single cryptographic algorithm verification at the BAH level (illustrated as a letter in Graph 4). Therefore, simultaneous validation of traditional and PQC-based signatures was not feasible within the existing configuration framework. Enabling such hybridisation would have required additional development effort, time and resources beyond the current project scope. Therefore, it was decided to test only PQC at the BAH level.

As illustrated in Graph 4, the payment message was sent with a PQC digital signature at the header of the letter (BAH level) but not in the envelope which contains the data exchange protocol (DEP level). As ESMIG is not currently configured to simultaneously accept a PQC algorithm at the message level and a traditional algorithm at the envelope level, a new software component was developed specifically for PQC signature verification. With this approach, the integration of new cryptographic methods was achieved without modifying ESMIG's current architecture.

As shown in Graph 4, the incoming flow was split into two distinct parts: a traditional signature verification software component capable of verifying traditional RSA signatures and a PQC signature verification software capable of managing PQC digital signatures on incoming messages. The outbound flow was signed using traditional RSA encryption only. These configurations allowed compatibility with existing system requirements, while simultaneously enabling the validation of new verification processes associated with the PQC signature. A dual-path approach showed PQC implementation capabilities without disrupting the broader system's RSA-based operations. Further tests will need to be conducted to verify the PQC digital signature both at the BAH and DEP levels.

Because configuring the HSM was not in the scope of the project, the signature verification software was configured using raw key pairs instead of conventional digital certificates. While this approach facilitated rapid prototyping with limited complexity for key management setup, it also constrained testing to standardised certificate-based validation procedures. As a result, essential security features such as certificate validity periods and hierarchical trust chain validation will need to be tested in future experiments in order to maintain compliance and auditability.

A further challenge involved a version mismatch between the vendor software and the existing Java runtime environment. In the experimental system, a temporary workaround was implemented to bypass this versioning conflict, allowing the tests to proceed without necessitating a full upgrade of the ESMIG environment. Versioning incompatibility is an expected issue that systems will encounter when migrating to post-quantum cryptography.

4. Testing and key findings

4.1. Test scenarios

For functional testing, two main test scenarios were defined: a positive scenario with a valid signature and a negative (or "fault injection") scenario with an invalid digital signature. In addition, performance and interoperability were assessed.

Positive test scenario: PQC signature with correct private key

In the positive test scenario, a liquidity transfer (camt.050 message type) was signed using a valid PQC private key. This scenario aimed to verify correct functioning of the digital signature generation, transmission and validation under different cryptographic configurations and message volumes. First, multiple individual messages were sent by central banks, followed by a bulk of 50 signed messages. The messages were expected to be processed by the system and be validated by ESMIG. In response, messages were expected (camt.025) acknowledging correct reception.

As expected, the absence of a corresponding digital certificate in the CRDM module prevented the system from completing the settlement process. While unrelated to signature validation, this behaviour confirmed the system's reliance on centralised certificates even when using PQC.

Fault injection test scenario: Rejected PQC signature with incorrect private key

In the negative test scenario, the message was signed using a knowingly incorrect PQC private key, thereby producing an invalid digital signature. The scenario aimed at testing the system's resilience and error handling capabilities. The system was expected to identify invalid keys and appropriately reject messages that were cryptographically compromised. ESMIG was expected to reject the message by sending a standardised admi.007 error message, correctly indicating that the signature could not be verified.

This test scenario was critical to confirm the ability of the system to maintain current and future robust security defences. Verifying that the integrity of the system remains safeguarded after being reconfigured with PQC is an important step when migrating to new cryptographic protocols.

Performance tests

The primary objective of the performance study was to assess the potential impact of PQC for payment systems with a particular emphasis on initiating the implementation and testing of new cryptographic protocols.

Tests were configured to evaluate the performance impact when implementing PQC compared with traditional cryptography. The intention was to evaluate the system's ability to handle a high volume of post-quantum digital signature operations within a given time frame. Estimating the resources required for the entire process, including key generation, encapsulation, decapsulation, signing and verifying, was out of scope. Only the duration of the verification step was systematically measured and documented. For that purpose, metrics about different parameters such as time stamps and log files with size information were collected.

Interoperability

Additionally, for interoperability to be tested during the technical experiment, each participant implemented a different cryptographic library, either provided by a solution vendor or selected from existing open source solutions. All solutions were required to communicate, proving an adequate level of interoperability in the system.

4.2. Test results and key findings

All test cases were successfully executed and results met expectations, providing strong confirmation of both functional behaviour and security resilience under PQC implementation (Table 1)

Table 1 – Tests performed

	Test	Expected result	Observed result	Pass/fail
Positive test scenario	Send a payment message with RSA	Payment message can be processed	Payment message successfully processed	Pass
	Send a payment message with PQC	Payment message can be processed with a PQC digital signature	Payment message successfully processed	Pass
Fault injection scenario	Send a message with invalid PQC signature	Verify the system rejects invalid digital signature	Invalid digital signature successfully rejected	Pass
Performance	Send a bulk of 50 messages with RSA	Measure time to verify traditional digital signature	Measurements in accordance with normal processing	Pass
	Send a bulk of 50 messages with PQC	Measure time to verify signature	Time required to verify the digital signature was higher with PQC, as expected	Pass
Interoperability	Send payment messages between payment system participants with different PQC solutions	Each participant implements different PQC solutions either from vendor or open source	Interoperability was verified	Pass

Functional results

The liquidity transfer message signed with a correct PQC signature (ie a positive test scenario) was successfully processed by the system and validated by ESMIG.

Due to the absence of a corresponding digital certificate in the T2 static data, the system could not complete the process until settlement. This behaviour was in line with expectations and confirmed the system's reliance on centralised certificate data even when using PQC.

When the private key file was replaced by an unknown key (ie a negative test scenario), the message led to verification errors on ESMIG side (admi.007). The liquidity transfer message with the incorrect private key was successfully rejected. By the generation of appropriate error responses, the system validated:

- Its resilience in maintaining security standards when confronted with potentially malicious or corrupted payment instructions; and
- The robustness of its security controls following the integration of the PQC verification bypass mechanism.

Performance

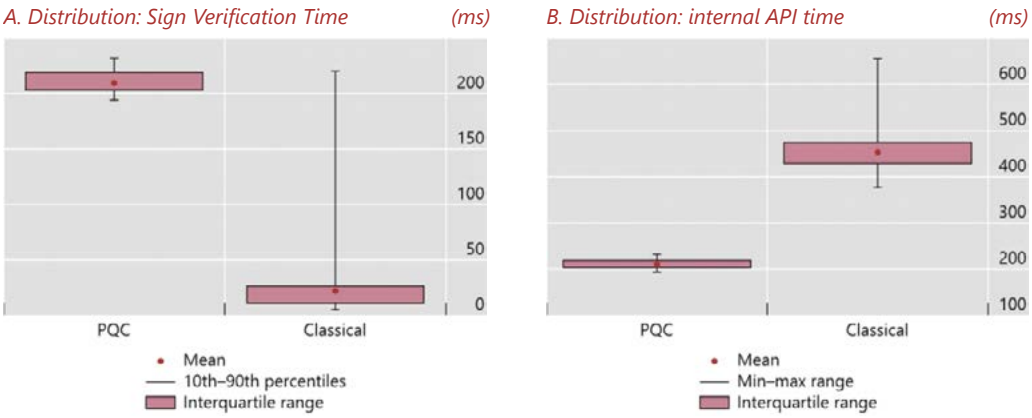
Performance measurements revealed significant differences between PQC and traditional cryptography. The time required for PQC signature verification was significantly higher, by at least an order of magnitude, compared with traditional cryptographic methods. This reflects the increased computational complexity associated with post-quantum algorithms. As illustrated in Graph 5, the average verification time for PQC signatures was 209.9 milliseconds (ms), whereas traditional cryptography achieved the same tasks in just 28.1 ms. This gives an indication of the potential need for more computing power. The project team acknowledged the need for additional testing, including of other system components.

On the client side, the impact was not measured as an HSM was not utilised. Performance can significantly vary depending on the type of HSM used, as manufacturers implement different hardware architectures.

Impact of PQC on system performance

Graph 5

In milliseconds



Execution times for verification of CRYSTALS-Dilithium.

From a cost standpoint, it is widely recognised that the larger key sizes associated with PQC may impose greater demand on hardware as additional storage capacity will be needed. This will depend on the use case and additional tests need to be performed using the full range of existing IT systems.

Interestingly, application programming interface (API) response times were lower with PQC than with traditional cryptography. This API is internal to T2. It relates to the time needed for ESMIG to send a request to the signature verification software. For the technical experiment, the request was simplified due to the use of software-generated keys. It is expected that in production environments, the request would take substantially more time. A precise quantification of this increase will require targeted performance benchmarking under deployment conditions in which all system components embed PQC cryptography. Further testing would need to include certificates operated by an HSM and not only software generated keys.

Additional findings

One important finding of the Leap technical experiment is the dependency on solution vendors. Successful migration will be conditioned by effective anticipation of vendor solution updates. A proactive approach will be necessary, involving dialogue with each vendor to make sure their roadmaps align with migration plans.

An initial objective of the experiment was to perform tests with hybrid cryptographic protocols. According to NIST IR 8547, hybrid cryptographic solutions are recommended during the transition to PQC (NIST (2024a)). The final decision on hybrid adoption is left to implementers and cyber security agencies, based on their risk assessment and operational needs. Before starting the experiment, a study was performed to assess whether hybrid solutions could be implemented in T2. The findings of this study indicated that substantial evolution of the system will be required, as hybridisation was not envisaged in the original cryptographic design. Payment systems will need to be made more agile before or as part of the PQC migration.

Among the various challenges of testing, interoperability proved to be surprisingly straightforward, highlighting the value of prior interoperability tests, for example by the National Cybersecurity Centre of Excellence (NIST (2023)). However, other aspects such as performance or cryptographic agility still need more investigation. Further testing will be required to assess performance across additional payment flows and to evaluate compatibility with other system components. Involving more organisations will be critical to ensure that all payment system participants achieve a straightforward migration.

5. Conclusion and next steps

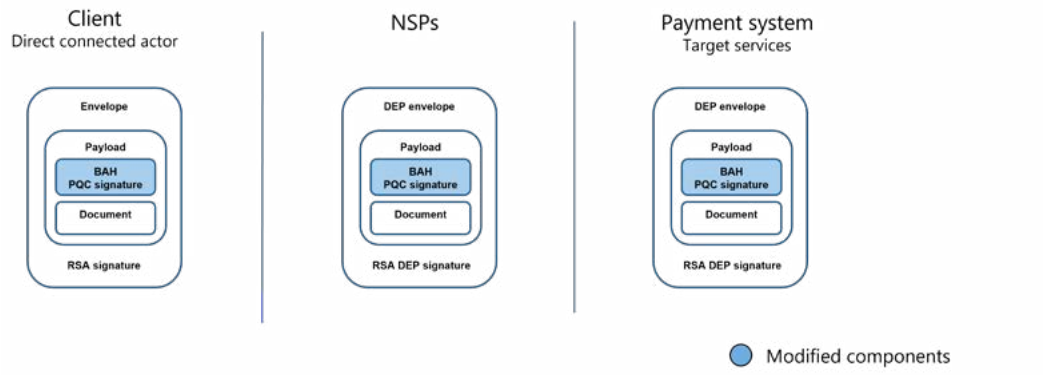
Project Leap Phase 2 confirmed that post-quantum cryptography can be successfully implemented in payment systems. The experimental system accepted and processed liquidity transfers with valid post-quantum signatures, while it appropriately rejected messages with invalid signatures – thereby preserving the overall integrity and trustworthiness of the transaction environment. The project's findings will contribute to roadmap development, risk mitigation and the broader transition to post-quantum security standards.

Besides demonstrating functional correctness, the Leap experiments have resulted in learnings related to performance, interoperability and cryptographic agility. In terms of performance, the experiments highlighted that post-quantum cryptography leads to significantly higher processing time than traditional algorithms, which will need to be taken into consideration when planning migration. Another important conclusion relates to the ability of systems to accept hybrid cryptographic protocols. The Leap Phase 2 experiment showed that existing systems need substantial time and resources to develop their ability to accept hybrid cryptographic solutions. Such limitations will need to be identified and addressed before migrating systems to post-quantum cryptography.

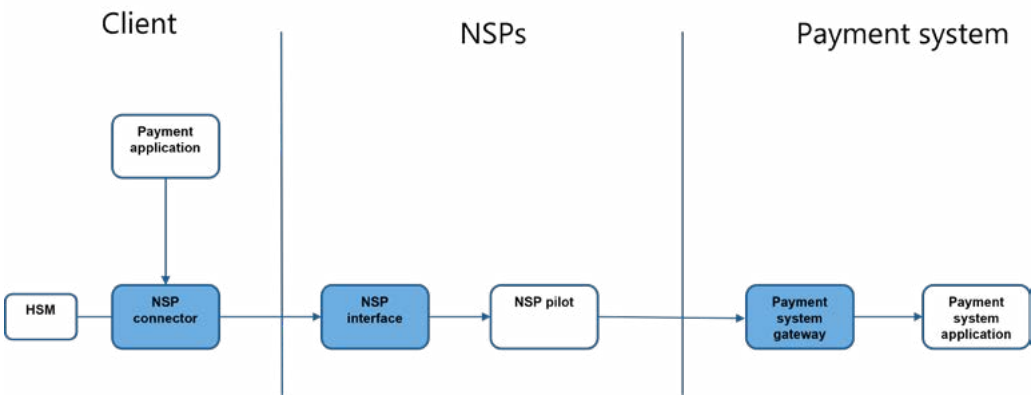
Payment systems are complex and highly interconnected with multiple stakeholders. Additionally, the payment ecosystem is characterised by a diversity of different configurations. Project Leap Phase 2 involved three distinct central banks, each with its own internal architecture, thereby necessitating tailored adaptations to accommodate the specific configurations of each entity. The same observation applies for NSPs. Project Leap is a case in point – migrating payment systems will require long-term planning, adequate resource allocation and the coordination of numerous stakeholders. It is time to align quantum-readiness roadmaps across the financial ecosystem and start the migration process to ensure the continued integrity and stability of the global financial system.

6. Annex A

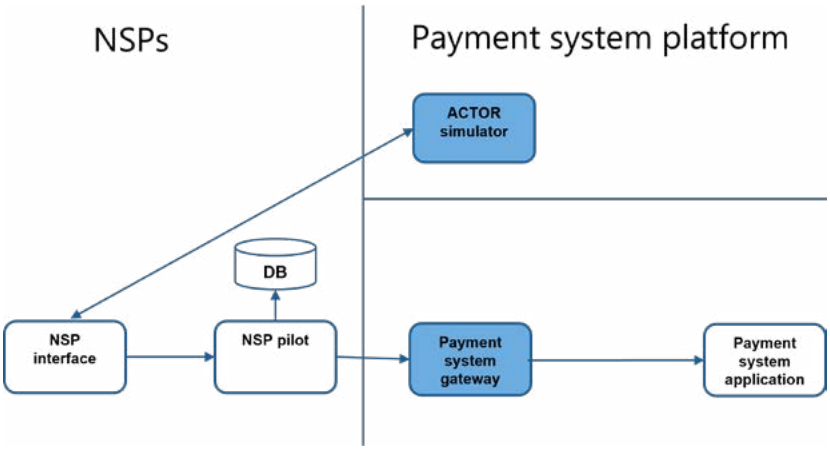
Detailed structure of the payment message



Payment message flow with NSP connector within the central bank IT system



Payment message flow with NSP connector outside the central bank IT system



7. References

Andriani, C, L Bencivelli, A Castellucci, M De Santis, S Marchetti and G Piantanida (2024): "The quantum challenge: implications and strategies for a secure financial system", *Bank of Italy Occasional Papers,* no 877, October.
www.bancaditalia.it/pubblicazioni/qef/2024-0877/QEF_877_24.pdf?language_id=1

Auer, R, D Dodson, A Dupont, M Haghighi, N Margaine, D Marsden, S McCarthy and A Valko (2025): "Quantum-readiness for the financial system: a roadmap", *BIS Papers,* no 158, July.
www.bis.org/publ/bppdf/bispap149.pdf

Auer, R, A Dupont, L Gambacorta, J S Park, K Takahashi and A Valko (2024): "Quantum computing and the financial system: opportunities and risks", *BIS Papers*, no 149, October.
www.bis.org/publ/bppdf/bispap149.htm

BIS Innovation Hub (BISIH), Bank of France and Deutsche Bundesbank (2023): *Project Leap: quantum-proofing the financial system,* June.
www.bis.org/publ/othp67.htm

Bank of France (2024): Banque de France and Monetary Authority of Singapore conduct groundbreaking Post-quantum Cryptography experiment to enhance communication security", press release, 5 November.
www.banque-france.fr/en/press-release/banque-de-france-and-monetary-authority-singapore-conduct-groundbreaking-post-quantum-cryptography

——— ((2024): *Post-quantum cryptography: securing digital communications between Banque de France and Monetary Authority of Singapore,* November.
www.banque-france.fr/system/files/2024-11/BDFxMAS%20report%20final.pdf

Bucciol, E and P Tiberi (2023): "Quantum safe payment systems", *Markets, Infrastructures, Payment Systems,* no 35, June.
www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2023-035/N.35-MISP.pdf?language_

Butler, A and A Herman (2023): Prosperity at risk: *the quantum computer threat to the US financial system, Hudson Institute*, April.
s3.amazonaws.com/media.hudson.org/04.03.2023+_Butler_Prosperity_at_Risk_Quantum_Report.pdf

Castellanos, S (2020): "Visa, JPMorgan are already preparing for potential quantum cyberattacks", *The Wall Street Journal*, 9 October.
www.wsj.com/articles/visa-jpmorgan-are-already-preparing-for-potential-quantum-cyberattacks-11602255213

Cybersecurity and Infrastructure Security Agency (CISA) (2022):
"CISA announces post-quantum cryptography initiative", press release, 6 July.
www.cisa.gov/news-events/news/cisa-announces-post-quantum-cryptography-initiative

Ducas, L, E Kiltz, T Lepoint, V Lyubashevsky, P Schwabe, G Seiler and D Stehlé (2021):
CRYSTALS-Dilithium: algorithm specifications and supporting documentation,
version 3.1.
pq-crystals.org/dilithium/data/dilithium-specification.pdf

Eisenbach, T, A Kovner and M Lee (2020): "Cyber risk and the US financial system:
a pre-mortem analysis", *Federal Reserve Bank of New York Staff Reports*, no 909.
www.newyorkfed.org/research/staff_reports/sr909

European Commission (2025): *Quantum Europe strategy,* July.
digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy

Europol (2025): *Quantum safe financial forum: a call to action.*
www.europol.europa.eu/cms/sites/default/files/documents/Quantum-safe-financial-forum-2025.pdf

Federal Office for Information Security (BSI) et al (2025): *Securing tomorrow, today: transitioning to post-quantum cryptography, joint statement*, June.
www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf?__blob=publicationFile&v=3

Ferreira, R, P Ripper, R Veríssimo and A Cavalcante (2022): *Neto post-quantum cryptography methods applied to the Brazilian instant payment system (Pix): a feasibility study*, Central Bank of Brazil and Brazil Quantum.
fenasbac.com.br/documentos/quantum-cryptography-pix-en.pdf

Finextra (2024): *HSBC and PayPal tackle quantum-safe cryptography in payments.*
www.finextra.com/newsarticle/44060/hsbc-and-paypal-tackle-quantum-safe-cryptography-in-payments

G7 Cyber Expert Group (2024): *Statement on planning for the opportunities and risks of quantum computing,* September.
home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf

Gibson, C (2024): *Quantum cyber threats are likely years away. Why – and how – we're working today to stop them, Mastercard,* March.
www.mastercard.com/global/en/news-and-trends/perspectives/2024/quantum-cyber-threats-are-likely-years-away-why-and-how-we-re-working-today-to-stop-them.html

Gidney, C (2025): V*How to factor 2048 bit RSA integers with less than a million noisy qubits*, arXiv:2505.15917v1.
arxiv.org/pdf/2505.15917

Grassl, M, B Langenberg, M Roetteler and R Steinwandt (2015): *Applying Grover's algorithm to AES: quantum resource estimates,* arXiv:1512.04965v1. arxiv.org/pdf/1512.04965

ISED-ISDE (2023): *Canada's National Quantum Strategy.* ised-isde.canada.ca/site/national-quantum-trategy/sites/default/files/attachments/2022/NQS-SQN-eng.pdf

Jackson, K, C Miller and D Wang (2023): "Evaluating the Security of CRYSTALS-Dilithium in the Quantum Random Oracle Model" in M Joye and G Leander (eds), *Advances in cryptology – Eurocrypt 2024*, Springer. nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

Kazmi, R, D-P Le and C Minwalla (2023): "Privacy-preserving post-quantum credentials for digital payments", *Bank of Canada Staff Working Paper,* June. www.bankofcanada.ca/wp-content/uploads/2023/06/swp2023-33.pdf

Monetary Authority of Singapore (MAS) (2024): "Advisory on addressing the cybersecurity risks associated with quantum", *Circulars*, no 1, February. www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum

National Cyber Security Centre (NCSC) (2020): "Preparing for quantum-safe cryptography", *NCSC White Paper,* November. www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf

National Institute of Standards and Technology (NIST) (2023): "Migration to post-quantum cryptography quantum readiness: testing draft standards", *NIST Special Publication,* December. www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf

——— (2024a): "Transition to post-quantum cryptography standards", *NIST Internal Report*, no 8547, November. nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

——— (2024b): *Announcing approval of three Federal Information Processing Standards (FIPS) for post-quantum cryptography,* August. csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

——— (2025): NIST selects HQC as fifth algorithm for post-quantum encryption, 11 March. www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

Network and Information Systems (NIS) Cooperation Group (2025): *A coordinated implementation roadmap for the transition to post-quantum cryptography.* digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Contributors

BIS Innovation Hub Eurosystem centre

Angela Dupont (Project Lead and Adviser)
Raphael Auer (Centre Head)
Andras Valko (Deputy Centre Head)
Anh Trung Nguyen (Adviser)
Charlotte Mellor (Operational Manager)
Violeta Vuletic (Data Scientist)

Bank of Italy

Marco Perelli (IT manager)
Pietro Tiberi (IT Operations Manager)
Donatella Bernabucci (IT Communication Manger)
Gianluca Lepore (IT expert)

Bank of France

Alexandre Le Douaron (Deputy Head of Le Lab)
Christian Leroux (Functional Manager)
Diana Sturza (Deputy Functional Manager)
Dan Toledano (Market Infrastructure Expert)
Nicolas Margaine (Cryptography Expert)
David Viatgé (Cryptography Expert)
Pierre Pouliquen (Cryptography Expert)
Baptiste Demets (Project Manager)
Celia Hammouche (Business Analyst SWIFT)
Gervais Bultel (Project Manager)

Deutsche Bundesbank

Norbert Stuckmann (Head of Division, DG Information Technology)
Johannes Rogowsky (DG Strategy & Innovation)
Philipp Neumann (DG Information Technology)
Eldin Delić (DG Strategy & Innovation)
Ulrich Tonner (DG Payments & Settlement Systems)

Nexi-Colt

Diego Trombetta (Secure Messaging Product Manager)
Davide Corti (Head of Secure Messaging Services)
Alessandro Roveda (Head of Network Services Solutions)
Luca Biancardi (Chief Security Officer)
Mirko Gattulli (Secure Messaging Solution Architect)

Swift

Isabelle Noblesse (Head of Product Security Roadmap & Innovation)
Arnauld Boulnois (Head of Messaging and MI Services)
Gauthier Helin (Head of On Prem Products Engineering)
Parag Ghodgaonkar (Head of SwiftNet)
Sajid Muhammad (Technical Authority)
Zong Guo (Cryptography Expert)
Vlad Kleban (Developer)

Project observers

Miguel Angel Pena (Bank of Spain)
Corina Wenzel (European Central Bank)
Valerie Saintot (European Central Bank)

Acknowledgements

The authors are grateful to Beju Shah and Alonso Carrillo for reviewing this report and providing extremely valuable feedback.

Bank for International Settlements (BIS)

ISBN 978-92-9259-918-8 (online)