LE LAB Banque de France

November 2022

REPORT ON THE "POST-QUANTUM" TRIAL

POST-QUANTUM DATA EXCHANGE SECURITY SOLUTION

1 INTRODUCTION

While it remains unclear whether quantum computers will actually be available for use with operational applications in the next decade, the prospect is growing increasingly credible, as successive announcements by major tech players show that the quantum development timetable is picking up speed.

Quantum computing has the potential to bring material improvements in areas of particular interest to the Banque de France, such as macroeconomic and financial modelling, processing efficiency and artificial intelligence. It could hold the key to tackling problems that have been out of reach until now, while slashing execution times and energy consumption relative to existing computing applications. For these reasons, the Banque de France is paying close attention to quantum technology and actively monitoring its development.

However, it is acknowledged that the first practical applications of this technology will include large number factorisation and search functions, paving the way to break the algorithms that are widely used to encrypt and authenticate data exchanges and that are critical to the security of online communications and IT infrastructures. These algorithms play a vital role in protecting communications over the internet as well as IT infrastructures such as secure websites, virtual private networks (VPNs), payment solutions, identity management infrastructures, digital signatures, blockchain and more.

For this reason, the quantum revolution poses a systemic threat to data integrity and security. The authorities responsible for information security in most industrialised countries, including France's *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI – National Agency for Information System Security), share this concern.

The Banque de France, which itself uses cryptographic solutions in its activities, can ill afford to ignore the quantum threat. More broadly, under its financial stability responsibilities, it cannot overlook the potential future impact of quantum technology on the security of financial exchanges and public confidence in the digital economy.

The Banque de France therefore conducted a recent trial of post-quantum communications protection solutions to assess their capacity to be integrated in existing information systems. In line with ANSSI recommendations, it adopted a hybrid approach featuring backward compatibility with current standards and also prioritised crypto-agility by working with several algorithms currently under selection by the US National Institute of Standards and Technology (NIST) or recommended by ANSSI in France or Germany's Federal Office for Information Security (BSI).

In January 2022, the Banque de France launched the trial, which ran to July and which involved deploying a library of quantum-robust algorithms satisfying these requirements.[1] The solution was initially tested on data exchanges protected by an IPsec VPN with a complete quantum-resistant trust chain functioning in hybrid mode (authentication, key exchange for encryption and HSM).

The Banque de France collaborated on the project with CryptoNext Security, a start-up founded in 2019 as spin-off from INRIA, Sorbonne University and the CNRS. Through the software products that it has developed, CryptoNext Security brought to the project its command of innovative quantum-resistant algorithms and hybridisation of security protocols, as well as valuable technical assistance in deploying the solution within Banque de France infrastructures.

The successful trial has enabled the Banque de France to gain an understanding of post-quantum cryptography technologies. As such, it will form part of the Bank's strategic policy of developing the institution's communication and information security systems on an ongoing basis, by ensuring that the Banque de France is ready to respond to the quantum threat if and when it arises.

1 The Banque de France has successfully experimented with CryptoNext Security post-quantum security technologies | Banque de France (banque-france.fr)

2 WHY WAS THIS TRIAL CONDUCTED?

2.1 WHAT IS THE "QUANTUM THREAT"?

All data exchanged on the internet are protected using supposedly-safe cryptography algorithms. The most widely used are RSA (and its more recent alternative, elliptic-curve cryptography), which is asymmetric (based on a public key and a private key that are mathematically and closely linked), and AES, which is symmetric (just one key, which is therefore necessarily private but shared by the issuer and the recipient). These algorithms may be used alternatively or to complement each other.

Example:

when you use a web browser to visit a secure website, the site sends the browser a digital certificate (typically based on the RSA algorithm) that contains the information needed for the browser to authenticate the site (notably the asymmetric encryption method applied and the site's public key), by using the public key to verify the signature applied to the data by the site with the certificate's private key.

Following the authentication stage, an asymmetric key exchange algorithm such as Diffie-Hellman allows the browser and the website to exchange a shared symmetric key, enabling exchanges to be encrypted with the selected encryption algorithm, e.g. AES.

Today's most commonly used public key encryption systems (RSA, elliptic curve), which are based on mathematical problems that are unsolvable, at least in a reasonable time, even for the fastest conventional computers, ensure that exchanges stay secure.

But a quantum computer with sufficient power (expressed in number of qubits) and able to execute a huge number of calculations simultaneously using a different technology from that of the machines currently available, could solve these problems far more quickly.

Algorithms have already been identified that are capable of attacking the main security systems in use today. For example, the Shor algorithm can be used to break asymmetric encryption (RSA and elliptic-curve algorithms), while the Grover algorithm can crack symmetric encryption (AES).

The Shor algorithm has been at the root of the scientific community's strong interest in quantum computing since it was developed in 1994. The algorithms used in classic computing to factor numbers, and hence to attack RSA encryption, quickly become unusable as the complexity of the problem increases.[2] Used with a quantum computer, however, the Shor algorithm could break RSA encryption in polynomial time.

Since a quantum computer can make parallel calculations across all possible values between 0 and 2^n, the Shor algorithm could be used to mount an effective "brute force" attack on an asymmetric encryption key with a finite probability of obtaining the right answer, remembering that the solution can be simply (and therefore very quickly) and repeatedly tested to obtain the sought-after result.

A recent CEA-List paper confirmed the effectiveness of this algorithm, which had been impossible to verify until now owing to the lack of appropriate tools.[3]

2 The complexity of the problem increases exponentially with the number of bits in the public key.

3 https://www.cea-tech.fr/cea-tech/Pages/2022/logiciels-quantiques-une-implementation-de-l-algorithme-de-shor-verifiee-pour-la-premiere-fois-.aspx

As the algorithmic research currently stands, it is estimated that a quantum computer with 22 million noisy qubits[4] would be required to crack a 2048-bit RSA key.[5] However, in a paper released in September 2021, CEA researchers said that by adding quantum memory to the computer, the number of qubits required would come down to 20,000 or even 13,000 after optimisation.[6]

Keeping in mind that by 2023, based on the roadmaps of tech firms working in this area, the most powerful quantum computer will have at best 1,000 qubits (IBM Quantum Computing | Roadmap) and perhaps 10,000 by 2026, it will probably take years to build a computer capable of cracking RSA encryption in an acceptable timeframe, but it is impossible to say right now when this milestone will be reached.

In the case of symmetric key algorithms, the Grover algorithm can reduce the number of iterations to the square root of the key. For AES-128, therefore, the number is reduced to 2^64 (which may be treated as vulnerable to quantum computing power), while for AES-256-type keys, the number is still 2^128, which may be considered to be resilient to the cryptanalytic capabilities of a quantum computer.

2.2 POSSIBLE RESPONSES

One possible response would be to increase the size of the keys used in existing algorithms to make it harder to solve the mathematical problem of "breaking" the keys. Another alternative would be to increase the frequency with which keys are updated. However, while this might help initially to ward off the quantum threat, the respite would be short lived. We need to act now to consider other more sustainable responses to the issue of post-quantum communications security.

This leaves two potential avenues of response:

- Harness the power of quantum physics to exchange encryption keys securely, an approach known as quantum key distribution (QKD). Based on existing technology, QKD requires an extremely sophisticated command of the physical conditions of the key exchange, raising challenges for operational implementation;

- Use new key and/or data encryption mechanisms, whose cryptanalytic difficulty would exceed even the capabilities of quantum computing. This is post-quantum cryptography (PQC), which offers the benefit of being implementable using conventional computers.[7] PQC is the route that is most often taken because it is the most easily realisable. It was also the approach adopted by the Banque de France in its trial.

2.2.1 Which algorithms can be used in post-quantum cryptography?

In July 2022,[8] the NIST published an initial group of encryption tools (three to secure key exchanges and one for signatures) designed to withstand the potential of quantum computers. The four selected algorithms will be included in the NIST's PQC standard, which is set to be finalised in the next two years.

Each of the algorithms proposes a specific compromise between the various constraints, namely key and signature size, the complexity and hence the computing needs of the key exchange, and the security assurance level.

For key exchange, which is used particularly when secure websites are accessed, the NIST chose the CRYSTALS-Kyber algorithm. Its advantages include comparatively small encryption keys that two parties can exchange easily, and speed of operation.

For digital signatures, which are often used to verify identities in digital transactions or to sign documents remotely, the NIST selected CRYSTALS-Dilithium, FALCON and SPHINCS+.

4 Corresponding to 14,238 qubits, each occupying 1,568 physical qubits.

5 banegasPresentation.pdf (inria.fr) and Cornell University paper: [1905.09749] How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits (arxiv.org).

6 *Espace Presse - Avec une mémoire quantique, l'ordinateur quantique est 1 000 fois plus petit !* (cea.fr).

7 The term "post-quantum cryptography" is sometimes criticised as being ambiguous. A more appropriate expression would be "quantum-robust cryptography".

8 Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates | CSRC (nist.gov).

The reviewers noted the high efficiency of the first two. The NIST recommended CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but is valuable as a backup as it is based on a different math approach from that of the NIST's other three selections (hash functions rather than structured lattice problems).

Four additional key exchange algorithms are under consideration for inclusion in the standard. This would offer more than one algorithm for each use case in the event that one proves vulnerable.

The Supersingular Isogeny Key Encapsulation (SIKE) algorithm, which made it through the first four rounds of the NIST's competition, was recently cracked by researchers from the Computer Security and Industrial Cryptography (CSIS) group at Belgium's KU Leuven University, demonstrating again that the resilience of these algorithms over the long run remains to be proven.

Although the attack did not impact the first four algorithms chosen by the NIST in August for standardisation, which are based on completely different math problems from those of SIKE, it shows the need for researchers to keep testing these algorithms to identify vulnerabilities, while looking into other mathematical approaches to complement those already identified.

Given the uncertainty about whether algorithms will hold up, participants must be ready to switch quickly to a different algorithm if one is found to have a weakness, a quality referred to as "crypto-agility".

2.2.2 Recommendations by information security authorities

PQC is still in the research and development stage and therefore remains relatively immature. However, this lack of maturity cannot be used as justification for affected participants to put off thinking about their strategy to deal with the quantum threat, in line with recommendations issued by domestic and international information security authorities.[9]

The US Department of Homeland Security recently published a transition roadmap, which called among other things for an inventory to be drawn up of the most sensitive data in the public and private sectors.

France's ANSSI[10] recommends acting immediately to begin a gradual transition in order to build trust in post-quantum algorithms and their implementations, while ensuring that conventional pre-quantum security does not regress in the context of a hybrid approach.

A hybrid key establishment or signature mechanism combines application of a pre-quantum public key algorithm and a post-quantum algorithm. Hybridisation offers a way to leverage the robustness of the former to conventional attacks and the resistance of the latter to quantum attacks.

Since most post-quantum algorithms involve messages sizes that are far larger than those of existing pre-quantum schemes, the additional performance cost of a hybrid system is small compared with the cost of a post-quantum system alone. The ANSSI considers this to be a reasonable price to pay to ensure pre-quantum security that is at least on a par with that delivered by current standardised pre-quantum algorithms.

For symmetric primitives, the ANSSI recommends targeting a post-quantum security level consistent with the selected post-quantum algorithm, i.e. in practice at least the same level as AES-256 for block ciphers and SHA2-384 for hash functions.

As mentioned earlier, given the uncertainty over the robustness of post-quantum algorithms, which will persist as long as they have not experienced prolonged exposure to genuine attacks, ANSSI is recommending a crypto-agile approach. Besides the quantum threat, it is important not to overlook conventional attacks, which may also evolve and render some cryptographic mechanisms or key sizes obsolete. In practice, therefore, crypto-agility also means that cryptographic solutions must be able to cope with updates to cryptographic algorithms in order to respond to future recommendations and updates to standards.

FrodoKEM (Levels 3 and 5) is one of two post-quantum algorithms recommended by Germany's BSI as being cryptographically suitable for long-term confidentiality protection. A developer should be able to obtain security approval for a product implementing FrodoKEM in hybrid mode, irrespective of the NIST's decision on whether to include the algorithm in the first round of PQC standardisation.

9 Including ANSSI in France, BSI in Germany and ENISA for Europe.

10 ANSSI views on the post-quantum cryptography transition | National Agency for Information System Security.

2.3 THE QUANTUM THREAT AS VIEWED BY THE BANQUE DE FRANCE

As financial and non-financial exchanges go more paperless and more global, our economies depend on the robustness of the techniques that are used to protect communications and data by ensuring the authenticity and integrity of data and identities, i.e. authentication and signature algorithms.

2.3.1 For the Banque de France itself

Just like any entity that uses information technologies and particularly one that exchanges data on public networks with third parties, the Banque de France is exposed to disruptions affecting the confidentiality of its communications and data stored temporarily or permanently in encrypted form in external systems. Likewise, it is exposed to the threat that data transmitted today on networks with robust encryption could be captured by public or private parties with the intention of storing the information now and deciphering it later once available technologies permit.

Within the framework of the development strategy for our data and communication security systems, and without waiting for post-quantum technologies to become available, we can gain some respite by using AES-256 more systematically to encrypt cold data and by regularly increasing the size of RSA keys for our public key infrastructure (PKI).

Like all public and private participants, we must consider these constraints in our strategic road map for the development of our data and communications security systems in order to make an effective transition, based on:

- an exhaustive inventory of cryptography use in applications and infrastructures;
- the acquisition of communication infrastructures integrating new post-quantum technologies;
- an overhaul of the entire IS, starting with the most sensitive elements, for end-to-end integration of these technologies.

Note that some hybrid protocols are in the process of being standardised, particularly for TLS 1.3 and IKEv2. The need to protect data exchanges as quickly as possible AND the maturity level of these protocols prompted the Banque de France to trial a technical solution this year that could one day protect communications between different Banque de France locations and with partners.

2.3.2 For the finance industry

Perhaps more than any other sector of the economy, the finance industry exchanges vast amounts of data, whose confidentiality and integrity are critical to the confidence of participants and, ultimately, to financial stability.

Banks, insurers and other finance sector institutions are thus dependent on having totally secure communication channels, whether for bilateral data exchanges or when accessing the market infrastructure services, such as interbank communication networks, currency and financial instrument trading systems and securities settlement systems, that are vitally important to orderly financial services.

Asymmetric keys are widely used to protect these communications. Successful attacks on these algorithms would compromise mobile banking services, e-commerce, payment transactions, ATM cash withdrawals, and communications via virtual private networks, to name but a few.

Central banks, which are generally entrusted with responsibility for preserving financial stability, have a duty to monitor the operational robustness of the sector as a whole and its participants. As such, they are paying attention to the ability of participants to protect themselves against attacks targeting the security of their data and communications.

Furthermore, they must be mindful of the fact that outside the traditional, regulated financial world, DLT-based applications, which support popular digital assets such as Bitcoin and Ethereum, also use public key cryptography to keep transactions secure.

To anticipate the quantum threat at the level of the finance industry as a whole, once a stocktaking has been done of the cryptography techniques used by participants themselves and by suppliers, a structured plan should be developed to gradually deploy quantum-robust technologies, whilst ensuring coexistence with existing technologies during the migration period.

This plan, which would need to be drawn up at a sector level but also at an international level owing to the interconnectedness of financial centres, should be based on the recommendations of security authorities, including their calls for hybridisation and crypto-agility.

"It is important to take the lead, because the transition could be very lengthy, as we are talking about the integrity of encryption or signing software. It will take years for everyone to take this step. In fact, the biggest threat right now is that information currently in circulation could be stored so that it can be deciphered quickly once quantum

computers are available", says Damien Stehlé, a professor at ENS de Lyon, a leading French research and educational institution, and a member of the Parallel Computation Laboratory (Lip).

2.3.3 Goals of the Banque de France trial

With all of this in mind, the Banque de France's trial had three goals:

- Understand post-quantum technologies,
- Measure their level of maturity and hence the feasibility of an application in an operational solution,
- To this end, test the Bank's capability to integrate these technologies in its information system and assess their potential and limits, particularly from a performance perspective.

3 HOW?

The Banque de France established several framing principles for the trial and on this basis opted to seek for a solution that would:

- Match operational constraints as closely as possible,
- Involve all components of the security chain, including secure key storage,
- Implement best practices in keeping with the spirit of the recommendations issued by security authorities, including on robustness of the algorithms, hybridisation and crypto-agility,
- Be achievable in an experimental framework without the need for resources (particularly expertise) exceeding the institution's capacities.

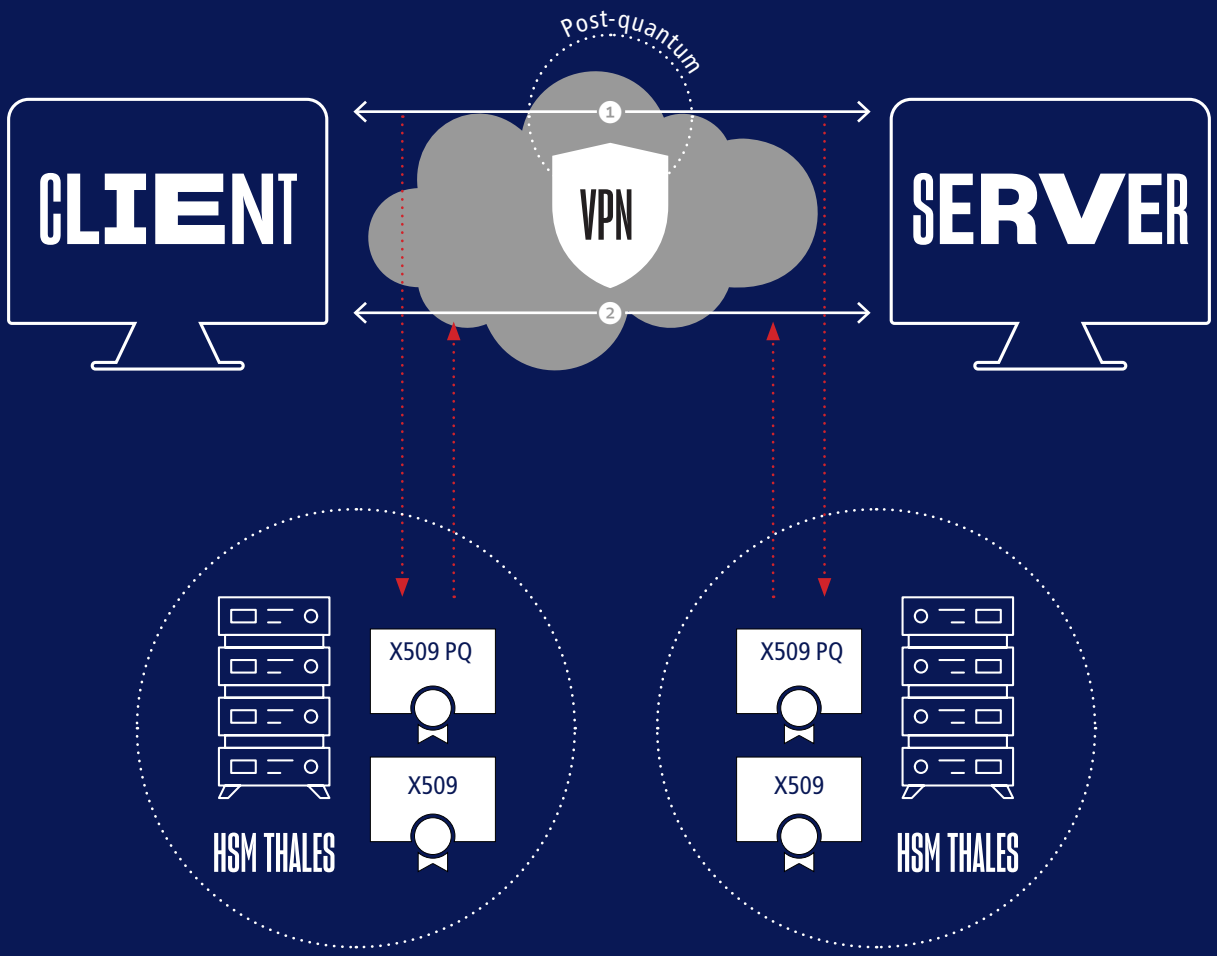
3.1 FUNCTIONAL ARCHITECTURE

Based on these principles, the Banque de France selected:

- An infrastructure project covering only the security of exchanges between network equipment and not involving applications, which would have made the project more complicated, entailed additional resources and entailed a risk of failure;
- And centred on the post-quantum security of symmetric key exchanges, reflecting the algorithms implemented by the NIST. The data exchange itself is protected by symmetric keys, specifically by the AES algorithm, which is proven, effective and deemed robust to quantum attacks (at least initially);
- Consequently, it was decided to test a post-quantum solution on a network exchange using an IPsec VPN that would make it possible:
    - to protect any existing type of data exchange at the level of the tunnel,
    - and, via the IKE protocol, to implement a hybrid solution based on conventional (Diffie-Hellman) and post-quantum algorithms;
- Among the post-quantum algorithms recommended by the NIST, the following were selected:
    - For authentication prior to key exchange: Dilithium,
    - For key exchange: **FRODO KEM** (selected in line with ANSSI recommendations), **KYBER**.

Two key exchange algorithms were selected to verify the solution's crypto-agility via a test to switch protection from FRODO to KYBER.

THE OVERALL OUTLINE OF THE SOLUTION WAS THEREFORE AS FOLLOWS:



1. IPSec PQ Authentication (+ RSA) + PQ Key Exchange (+ Diffie-Hellman)
2. Ciphertext exchange (AES)

3.2 TECHNICAL ARCHITECTURE

3.2.1 Hardware

The hardware architecture implemented is totally conventional, with virtual machines configured as follows:

- For the VPN server:
    - 2 CPU (Intel(R) Xeon(R) CPU E7540 @ 2.00GHz), 4GB RAM
    - Operating system: Debian Bullseye 5.10.120-1 (2022-06-09)
- For the VPN client:
    - 2 CPU (Intel(R) Xeon(R) CPU E7540 @ 2.00GHz), 4GB RAM
    - Operating system: Debian Bullseye 5.10.120-1 (2022-06-09)

Key storage and management were performed using standard Banque de France hardware (Thales Luna 7 NetHSM) connected to the server and client.

3.2.2 Software

A solution was selected from the post-quantum libraries supplied by CryptoNext Security SA to allow the Banque de France to leverage that company's experience in these technologies and their operational deployment.

Conversely, the option of developing a solution based on an open source library (Open Quantum Safe) was not taken due to the foreseeable load and the risks of problems or failure associated with a significantly more complex project.

Two configurations were implemented:

Configuration 1:

StrongSwan OpenSource IPsec VPN server and StrongSwan IPsec VPN client, the two parties being connected to a Thales Luna 7 NetHSM with a Functionality Module loaded with post-quantum libraries provided by CryptoNext Security.

Algorithms used:
- Signature: DILITHIUM
- Key exchange: FRODO level 5

Configuration 2:

StrongSwan OpenSource IPsec VPN server and TheGreenBow IPsec VPN client, with both parties using post-quantum libraries in software mode.

Algorithms used:
- Signature: DILITHIUM
- Key exchange: FRODO level 5 and Kyber

A series of shell scripts was developed to automate deployment of the configurations at the client and server levels, conduct data transfer tests in the tunnel, and retrieve and analyse logs obtained at the client, server and network levels.

4 FINDINGS

The project was successfully carried out, because it was used to deploy and test the post-quantum IPsec VPN solution defined above for the following configurations:

Configuration 1:

- StrongSwan IPsec VPN server connected to Luna 7 NetHSM
- StrongSwan IPsec VPN client connected to Luna 7 NetHSM

Configuration 2:

- StrongSwan IPsec VPN server
- TheGreenBow IPsec VPN client

The tests made it possible to ensure that the solution would work with different IPsec VPN clients (StrongSwan and TheGreenBow). Crypto-agility was tested by switching the Kyber and Frodo key exchange algorithms.

Several points to watch were identified:

- To obtain the maximum security level, the strict implementation of these solutions requires all components to be compatible with the post-quantum algorithms used (particularly the NetHSMs with Functionality Modules and the cryptographic libraries);

- Execution of the solution requires implementation of x509 post-quantum certificates (with Dilithium keys), alongside standard x509 certificates (with RSA keys). This makes it necessary to obtain post-quantum certificates from one or more trusted certification authorities (for the purposes of the project, these were specially adapted by the project team);

- Setting up the IPsec VPN tunnel connected to the NetHSM with a level 5 FRODO algorithm takes 4 to 5 seconds. This is not problematic for the tested use case, because time is taken only when the initial connection is made between the client and the server. But this lengthy time period would have to be re-examined for other use cases (particularly a TLS connection).

5 CONCLUSION

The success of the trial, which for now has been restricted to an internal perimeter within the Banque de France, indicates that to go deeper in the findings, the tests should be extended by involving third parties, so that key exchanges can be tested in a configuration that is even closer to real life, requiring the solution to be deployed in different technical contexts from that of the Banque de France, or potentially even exchanges between different solutions to test interoperability.

To this end, the Banque de France has established contacts with several French banking institutions with a view to planning information exchanges or bilateral tests.

The Banque de France will also shortly participate alongside the Deutsche Bundesbank in a project conducted by the Eurosystem centre of the BIS Innovation Hub[11] to test this type of solution in a cross-border framework.

All the results, which will be widely shared, will inform the Banque de France's strategic thinking on two levels:

- Its security systems development strategy and hence the investment roadmap for the renewal of communication and security equipment;

- Preparing the French financial sector (and the European sector in the context of the Eurosystem's financial stability responsibilities) to cope with a potential quantum threat.

11 The BIS Innovation Hub is a network of innovation centres in which the Eurosystem is participating through a centre with two facilities hosted by the Banque de France and the Deutsche Bundesbank.

LE LAB Banque de France

822393 BdF Dircom Studio Création – 11/2022