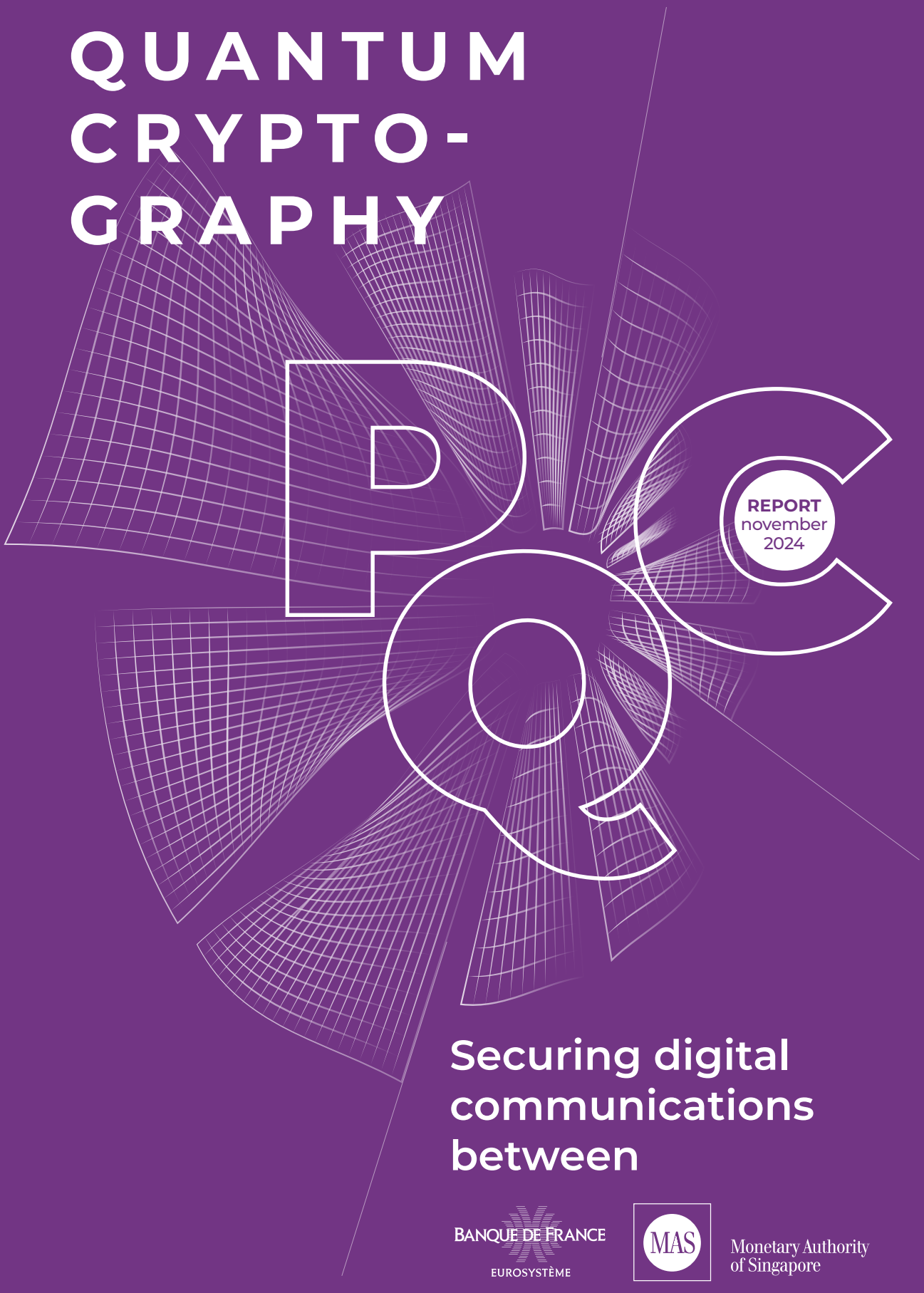
# POST-QUANTUM CRYPTO-GRAPHY




REPORT
november
2024

## Securing digital communications between

BANQUE DE FRANCE
EUROSYSTÈME

MAS
Monetary Authority of Singapore

# TABLE OF CONTENTS


EXECUTIVE SUMMARY ..... 4

INTRODUCTION ..... 6

BACKGROUND ..... 8

EXPERIMENTATION ..... 11

FINDINGS & DISCUSSION ..... 19

CONCLUSION ..... 21

ANNEXES ..... 23


"When we started working on the opportunities and risks posed by quantum computing more than two years ago, we quickly realised how impactful the quantum cyber-threat could be on the financial ecosystem and beyond. That is why, in Banque de France Le Lab, we focused on post-quantum cryptography (PQC) research and applications, with the conviction that this issue had to be dealt with at international level.

After having paved the way for the BIS Innovation Hub LEAP project with our successful VPN IPSec experiments, we were honoured to collaborate with the Monetary Authority of Singapore in order to provide joint crucial insights into PQC-secured applications, focusing on email messaging due to rising digital communication risks. This project underscores our common commitment to secure communications, and our shared belief that being quantum-safe can only be reached through cooperation.

Our successful exchange of encrypted and signed emails demonstrates PQC feasibility in existing infrastructure and highlights the need to adopt and foster crypto-agility standards. We extend our gratitude to Monetary Authority of Singapore for their commitment and look forward to further collaboration and advancements in PQC."

**Olivier Lantran**

Head of the Banque de France Innovation Centre

"The reality of quantum threats cannot be understated. Advancements in hardware and breakthroughs in algorithms may accelerate the arrival of Q-day, necessitating proactive measures to address quantum security challenges.

It is important to recognize that no entity is immune to quantum threats until the collective community elevates its defense. Preparation to be quantum-safe has to start now. Commencing trials, understanding the technology, and being mindful of the associated challenges are essential steps in strengthening our systems and networks against potential quantum vulnerabilities.

MAS has greatly benefited from the PQC experimentation with Banque de France and is grateful for this cross-continental collaboration opportunity. We look forward to advancing together in this critical quantum security endeavour."

**Damien Pang**

Executive Director (Data and Technology Architecture) and Deputy Chief FinTech Officer, Monetary Authority of Singapore

## EXECUTIVE SUMMARY

# Securing email communications through PQC algorithms

The Banque de France (BDF) and the Monetary Authority of Singapore (MAS) have collaborated on pioneering experimentation in post-quantum cryptography (PQC) to strengthen communication and data security in the face of quantum computing advancements. The joint initiative focuses on implementing quantum-resistant cryptographic algorithms, particularly for signing and encrypting emails at the application layer. The emergence of quantum computing poses a substantial threat to current encryption methods, necessitating proactive measures to safeguard financial and communication systems. The collaboration between BDF and MAS underscores the critical role of international cooperation in establishing a robust defense against quantum threats, fostering collective resilience and global financial stability.

The joint experimentation project by BDF and MAS specifically focuses on securing email communications through PQC algorithms, aiming to provide quantum-resistant signed and encrypted emails for enhanced confidentiality, authentication, and integrity. The successful implementation of PQC in widely used applications such as Microsoft Outlook combined with CryptoNext's PQC email plugin showcases the practical viability and effectiveness of these advanced cryptographic methods.

The experimentation employed a hybrid approach, combining the proven security of existing pre-quantum algorithms with the anticipated security of post-quantum algorithms, ensuring compatibility with current systems while preparing for impending quantum threats. The experimentation was conducted in strict compliance with the latest ANSSI recommendations and NIST strategic guidelines, aligning with ongoing standardisation processes.

**Aiming to provide quantum-resistant signed and encrypted emails for enhanced confidentiality, authentication, and integrity.**

Looking ahead, the focus extends beyond email transactions to investigate the use of post-quantum cryptography for critical financial transactions, possibly cross-border security over payment networks. This next step requires evaluating the viability, coordination, and limitations of integrating PQC security measures into the existing payment network infrastructure.

The collaborative efforts of BDF and MAS in pioneering PQC experimentation and the commitment to integrate quantum-resistant algorithms into real-world systems exemplify a strategic approach to evolving communication and information security systems, ensuring readiness against quantum threats and paving the way for a secure future.



BANQUE DE FRANCE EUROSYSTÈME

MAS Monetary Authority of Singapore

# POST-QUANTUM CRYPTO-GRAPHY

# REPORT

# INTRODUCTION

# 1

## Anticipating quantum threats

[1] **Quantum computing**
Unlike classical computers, which use bits to represent data as either 0 or 1, quantum computers use quantum bits or qubits, which can exist in multiple states simultaneously. This capability could enable quantum computers to solve certain complex problems much faster than classical computers.

The advent of quantum computing[1] presents a significant threat to current encryption methods, which rely on the computational complexity of tasks such as factoring large numbers or solving discrete logarithms. Foundational algorithms like RSA and Elliptic Curve Cryptography (ECC) are especially susceptible to this risk. Quantum algorithms, such as Shor's algorithm, are capable of efficiently breaking these cryptographic schemes by solving complex mathematical problems that are currently infeasible for classical computers.

This raises a major challenge because a large portion of today's sensitive data, including financial transactions and personal information, depends on these encryption methods for security. The "harvest now, decrypt later" scenario exacerbates this threat by allowing adversaries to intercept and store encrypted data now and awaits the development of quantum computers to decrypt it later. Thus, the quantum threat means that it is necessary to develop quantum-resistant encryption methods to safeguard data in the future quantum era.

The Banque de France (BDF) and the Monetary Authority of Singapore (MAS) recognise the importance of anticipating technological advancements and preparing for the quantum future. Both institutions are taking a forward looking approach and actively monitoring cryptographic developments.

In 2022, the National Institute of Standards and Technology (NIST) commenced the identification of four primary algorithms for standardisation. One is for key exchange, known as CRYSTALS-Kyber (renamed as ML-KEM[2]), and the other three are for signature: CRYSTALS-Dilithium (renamed as ML-DSA[3] ), SPHINCS+ (renamed as SLH-DSA[4]), and FALCON. On 13 August 2024, after undergoing extensive testing and public review, NIST has finally released a set of post-quantum encryption standards. They are ML-KEM, ML-DSA, and SLH-DSA.

In preparation for the release of these standards, BDF and MAS have been conducting tests since 2023 to gain expertise and understand the complexities of migrating to PQC. Specifically, BDF and MAS have conducted a PQC experimentation to secure email correspondences over the Internet by signing and encrypting emails at the application layer. This is done through a Microsoft Outlook plugin to demonstrate the feasibility and effectiveness of these advanced cryptographic methods in a real-world application.

**The importance of anticipating technological advancements and preparing for the quantum future.**

BDF and MAS are dedicated to maintaining the current systems until these standards are solidly established. The aim is to develop expertise and anticipate challenges in integrating these innovations in the existing environments. The success of this initiative is crucial for preparing both institutions for the post-quantum era.

[2] **ML-KEM** stands for Module-Lattice-Based Key-Encapsulation Mechanism Standard.

[3] **ML-DSA** stands for Module-Lattice-Based Digital Signature Standard.

[4] **SLH-DSA** stands for Stateless Hash-Based Digital Signature Standard.



QUANTUM-SAFE EXPERIMENT REPORT - 2024

BANQUE DE FRANCE EUROSYSTÈME
MAS Monetary Authority of Singapore

# BACKGROUND

## A pathway to ensuring secure communication

2

### 2.1. EXISTING WORK

In 2022, BDF initiated its journey into the PQC landscape with an internal project aimed at demonstrating the feasibility of implementing a complete security solution using quantum resistant algorithms. This experimentation focused on securing data exchange via an IPSec VPN tunnel. The results were promising, revealing that it is possible to integrate these advanced algorithms with minimal overheads, thereby maintaining system performance while enhancing security.

Building on the success of the internal project, BDF embarked on the LEAP I Project in 2023, in collaboration with the Bank for International Settlements Innovation Hub (BISIH) and Deutsche Bundesbank. This project aimed to install a security solution employing quantum-resistant algorithms for secure payments exchanged through an IPSec VPN tunnel. The primary objective was to measure the impact of these new algorithms on performance. The experimentation provided important insights into the practical implications of PQC in financial transactions, ensuring secure and efficient payment processes within a quantum-resistant framework.

MAS fully recognises the importance of addressing the cybersecurity risks associated with quantum computing and released an advisory in February 2024 highlighting the mitigating measures that financial institutions should consider. To highlight the importance of addressing the risks arising from





quantum computing, MAS has also embarked on its first cross-border collaboration with BDF to test the implementation of PQC encryption for email communications. This shared commitment underscores the collaborative approach both institutions are taking to ensure their readiness against quantum computing threats. By pooling resources and expertise, BDF and MAS aim to develop a resilient cryptographic defense paving the way for a secure future.

### 2.2. SCOPE OF THE EXPERIMENTATION

As part of the ongoing efforts to safeguard communication channels against the looming quantum computing threat, BDF and MAS have undertaken a critical joint experimentation project, specifically focused on securing email communications through Outlook. The initiative aims to provide quantum-resistant signed and encrypted emails to ensure their security during transmission over the internet.

BDF and MAS recognise email as a critical communication tool for exchanging sensitive and confidential information. Furthermore, as central banks, email is one of the main forms of communication. Hence, securing these communications is paramount to prevent unauthorised access and data breaches, making safeguarding emails a crucial task.

This project aims to enhance email security by using encryption to ensure confidentiality, and digital signature to authenticate the sender and ensure the integrity of the message. This dual security measure is essential for maintaining trust and reliability in electronic correspondence.

Lastly, this project aims to demonstrate the practical feasibility of implementing PQC in widely-used applications such as Outlook. This real-world application of PQC shows that these advanced cryptographic methods can be integrated into existing infrastructure with minimal disruption.

### 2.3. SELECTED ALGORITHMS

#### Choice of algorithms

In our cryptographic protocol design, CRYSTALS-Kyber and CRYSTALS- Dilithium are selected for key encapsulation/encryption and digital signatures respectively. CRYSTALS-Kyber is preferred due to its efficiency and strong security guarantees, making it an optimal choice for post-quantum cryptography.

Similarly, CRYSTALS-Dilithium, offers robust security for digital signatures and ensures reliable authentication in quantum-resistant systems.

#### Hybridisation

The need for a hybrid approach arises from the transitional nature of current cryptographic environments. While quantum-resistant algorithms are designed to be secure against quantum attacks, they are relatively new and less tested in real-world scenarios compared to classical algorithms like RSA. By using a hybrid approach, we combine the proven security of pre-quantum algorithms with the anticipated security of post-quantum algorithms. This ensures that even if one algorithm is compromised, the other will provide a layer of security, thereby enhancing the overall robustness.

In this experimentation, the digital signature is achieved by first signing with the RSA algorithm (sender's private key), followed by the concatenation of a CRYSTALS-Dilithium signature (also using sender's private key), thereby forming a hybrid signature.

Because there is no current standard for a hybrid S/MIME[5] exchange, we must decide on how to encapsulate the hybridisation. We determined that the encryption will be achieved by first encrypting with the RSA algorithm (recipient's public key), followed by encapsulating the result with CRYSTALS-Kyber encryption (also using recipient's public key).

[5] **S/MIME (Secure/Multipurpose Internet Mail Extensions)** is a widely accepted protocol for sending digitally signed and encrypted messages.

When performing sign and encrypt operations together, we follow the same order as S/MIME best practice by signing first and encrypting afterwards. This method ensures that the signer knows exactly what they are signing, which is crucial for verifying signer authenticity and maintaining message integrity.

By signing the plaintext message before encryption, the process guarantees that the content remains unaltered and that the sender's identity can be authenticated. Encrypting the signed message subsequently ensures its confidentiality, protecting it from unauthorised access during transmission.

### Compatibility with the standards

The experimentation was conducted in strict compliance with the latest ANSSI recommendations and NIST strategic guidelines.

Additionally, during the early stages of the project, we also reviewed guidelines from the leading institutions, including the Bundesamt für Sicherheit in der Informationstechnik (BSI), the European Union Agency for Cybersecurity (ENISA), the European Telecommunications Standards Institute (ETSI), and the Internet Engineering Task Force (IETF).

The choice of the final algorithms used was ultimately influenced by NIST's announcement in 2022, which revealed the first group of PQC algorithms (i.e. Kyber-768, Dilithium-5, etc) that were able to withstand the assault of a future quantum computer.





# EXPERIMENTATION

# 3

## A technical overview and scenario testing of the collaboration

[6] **Partnership** A partner in this experimentation, CryptoNext™ was founded in 2019 as a start-up after over 20 years of academic research at Sorbonne University (SU), INRIA, and CNRS in Paris.

[7] **PKCS#12** stands for Public Key Cryptography Standards #12. This file contains the user's private key and public key certificate. It allows the user to digitally sign emails and decrypt received encrypted emails.

[8] **Certificates** To send encrypted emails to others, you need the public certificates of the recipients. These certificates contain the recipients' public keys, which are used to encrypt the email content.

[9] **Certificate Authorities (CA)** are necessary to establish a chain of trust. The CA certificates verify the authenticity of the recipients' certificates and your own certificate. Importing the CA certificates ensures that the email client can validate the signatures on the certificates and trust them.

## 3.1. TECHNICAL SET-UP

The experimentation was conducted over the Internet, where BDF and MAS sent each other PQC-enabled emails. BDF used an internal server as their hosting infrastructure, while MAS used a private cloud.

Since the experimentation involved email transactions, mail domains were set up to route emails over public domains.

Microsoft Outlook was the chosen email client to fit CryptoNext[6]'s PQC email plugin (installation steps can be found in Annex A).

Each party had provided three users for the purpose of functional and exception handling tests.

PKCS#12 [7] files were imported for each user, along with the certificates[8] of the mail recipients and their corresponding Certificate Authorities[9] (CAs).

## SET-UP INFORMATION

| COMPONENTS | BANQUE DE FRANCE (BDF) | MONETARY AUTHORITY OF SINGAPORE (MAS) |
|---|---|---|
| 1. Hosting Infrastructure | Internal servers | AWS Cloud |
| 2. Virtual Machine Specifications | | |
| Email client | VM Windows 10 Enterprise<br>4CPUs, 8 GB ram, 160 GB | EC2 instance<br>t3.small, 2 vCPUs, 2 GB ram |
| Email server | Standard legacy infrastructure | EC2 instance<br>t3.medium, 2 vCPUs, 4 GB ram |
| 3. Email Client | Microsoft Outlook 2019<br>Version 1808 | Microsoft Outlook 2016<br>Version 2309 |
| 4. Email Plugin | CryptoNext QSMO v1.3.15-82<br>Quantum Safe Messaging for MS Outlook™ plugin | |
| 5. Mail Domain | test-banque-france.fr | masengage.com |
| 6. Mail Users | 2136-QUANTUMTEST1-UT@test-banque-france.fr | quantum@masengage.com |
| | 2136-QUANTUMTEST2-UT@test-banque-france.fr | kyber@masengage.com |
| | 2136-QUANTUMTEST3-UT@test-banque-france.fr | frodo@masengage.com |
| 7. PKCS #12 (P12) Certificate | P12 files of BDF's users | P12 files of MAS' users |
| 8. Public Key Certificate | Certificates of MAS' users | Certificates of BDF's users |
| 9. Certificate Authority (CA) Certificate | MAS' CA certificate | BDF's CA certificate |

Figure 1 | Setup Information



QUANTUM-SAFE EXPERIMENT REPORT - 2024

From a functional standpoint, the PQC email plugin is used to enable Microsoft Outlook to perform the following:

1. **Sign emails digitally** using CRYSTALS-Dilithium and RSA, and send to PQC-enabled recipient(s);
2. **Verify digital signatures** (signed using CRYSTALS-Dilithium and RSA) of email sent by PQC-enabled sender;
3. **Encrypt emails** using CRYSTALS-Kyber and RSA, and send to PQC-enabled recipient(s);
4. **Decrypt emails** (encrypted using CRYSTALS-Kyber and RSA) sent by PQC-enabled sender.

## QUANTUM-RESISTANT SIGNATURE

The following diagram illustrates BDF sending an email with a hybrid signature to MAS. In our use-case, we use the QSMO plugin to sign and validate, and not the Outlook built-in signature function (S/MIME).

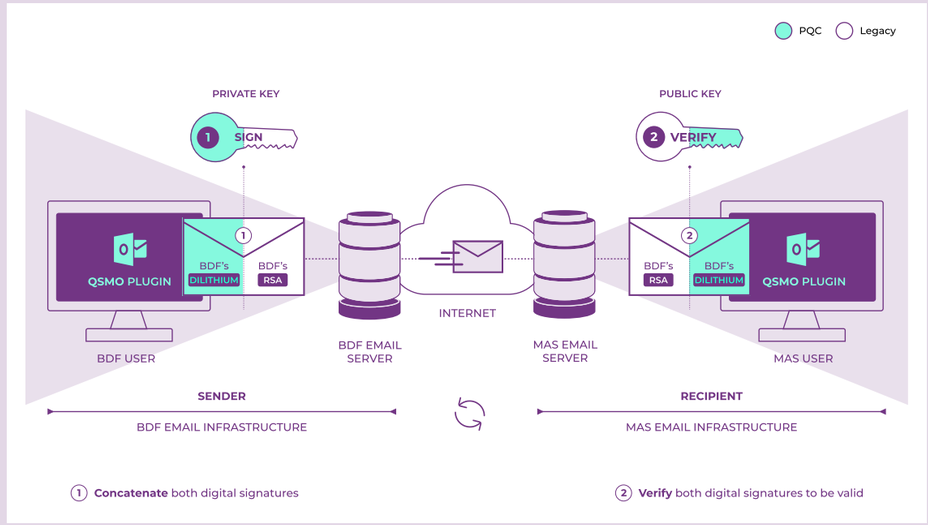



Figure 2 | Quantum-Resistant Signature Workflow

### ON BDF'S END

1. **Sign the plaintext email** separately using BDF's CRYSTALS-Dilithium private key and RSA private key. Concatenate both digital signatures and send them to MAS.

### ON MAS' END

2. **Verify both digital signatures** to complete sender verification.

## QUANTUM-RESISTANT ENCRYPTION

The following diagram illustrates BDF sending an email with hybrid encryption to MAS. In our use-case, we use the QSMO plugin to encrypt, and not the Outlook built-in encryption function (S/MIME).

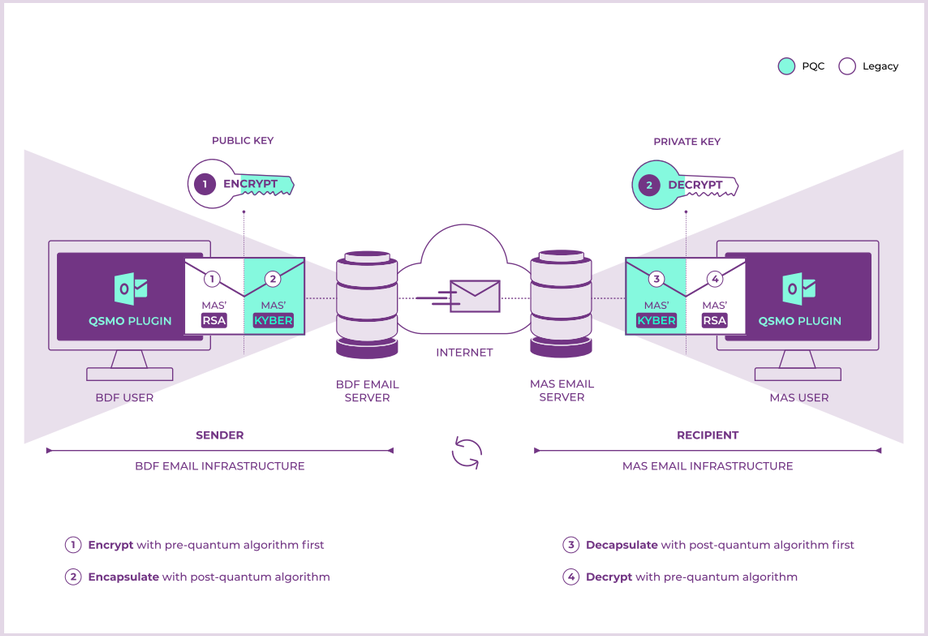



Figure 3 | Quantum-Resistant Encryption Workflow

### ON BDF'S END

1. **Encrypt the plaintext email** with MAS' RSA public key (pre-quantum algorithm).
2. **Encapsulate the resulting ciphertext email** with MAS' CRYSTALS-Kyber public key (post-quantum algorithm). Send the hybrid-encrypted email to MAS.

### ON MAS' END

3. **Decapsulate the hybrid-encrypted email** by decrypting with MAS' CRYSTALS-Kyber private key (post-quantum algorithm) first.
4. **Next, decrypt the resulting output** with MAS' RSA private key (pre-quantum algorithm) to complete the full decryption process.





## QUANTUM-RESISTANT SIGNATURE AND ENCRYPTION

The following diagram illustrates BDF sending an email with a hybrid signature and hybrid encryption to MAS. In our use-case, we use the QSMO plugin to sign, validate and encrypt, and not the Outlook built-in signature and encryption function (S/MIME).

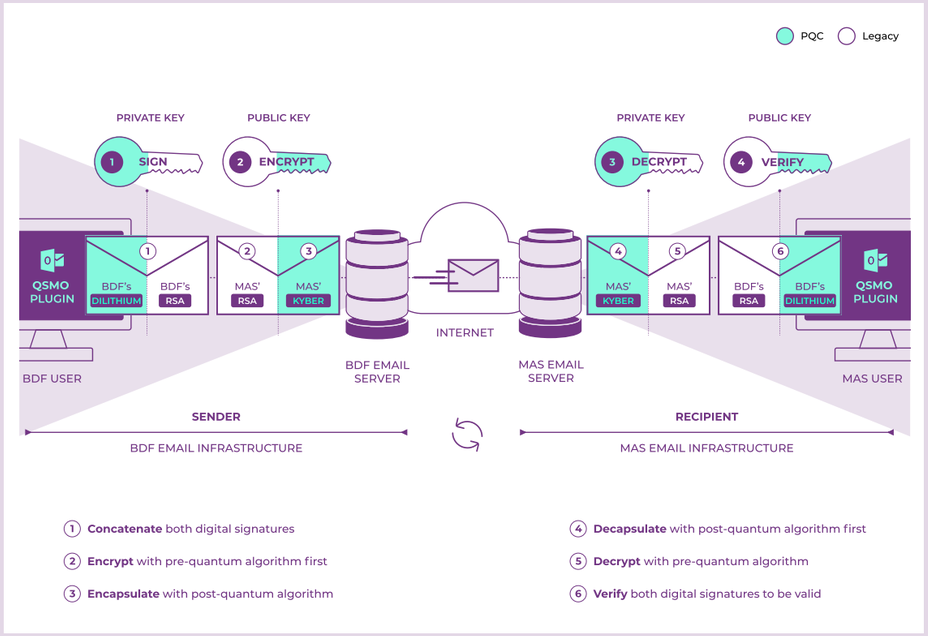



Figure 4 | Quantum-Resistant Signature and Encryption Workflow

### ON BDF'S END

1. **Sign the plaintext email** separately using BDF's CRYSTALS-Dilithium private key and RSA private key. Concatenate both digital signatures.
2. **Next, encrypt the plaintext email** and the two digital signatures with MAS' RSA public key (pre-quantum algorithm).
3. **Lastly, encapsulate the resulting ciphertext email** with MAS' CRYSTALS-Kyber public key (post-quantum algorithm). Send the hybrid-encrypted email to MAS.

### ON MAS' END

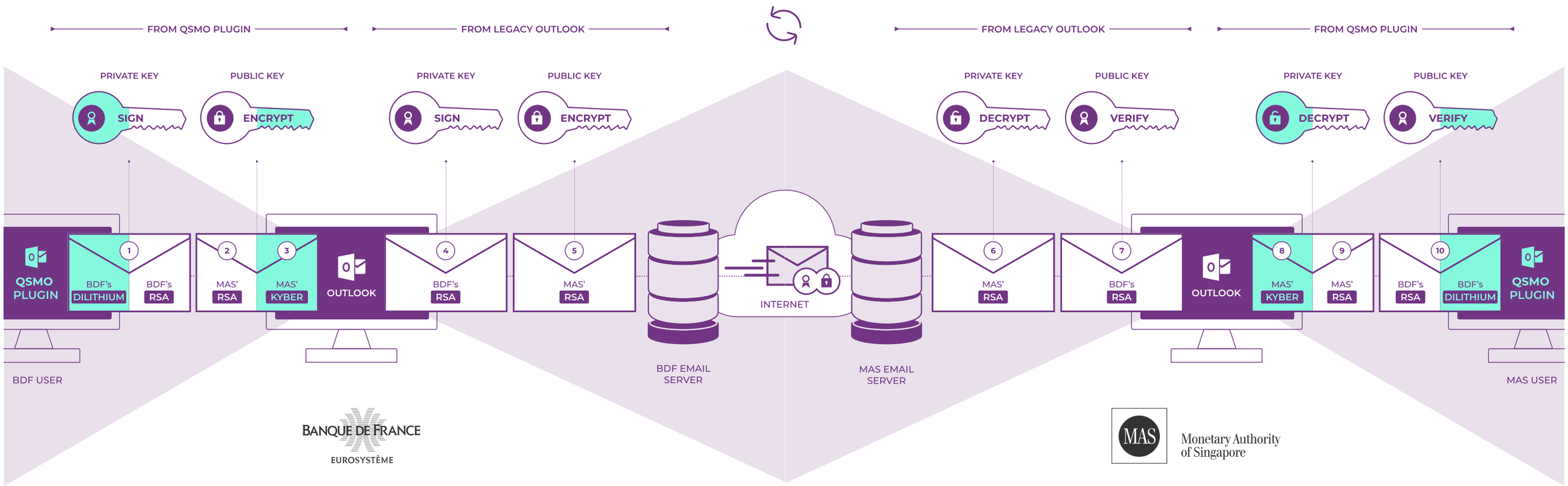
4. **Decapsulate the hybrid-encrypted email** by decrypting with MAS' CRYSTALS-Kyber private key (post-quantum algorithm) first.
5. **Next, decrypt the resulting output** with MAS' RSA private key (pre-quantum algorithm) to complete the full decryption process.
6. **Lastly, verify both digital signatures** to complete sender verification.

## QUANTUM-RESISTANT SIGNATURE AND ENCRYPTION

PQC Legacy

The following diagram illustrates BDF sending an email to MAS using a hybrid signature and hybrid encryption. In this scenario, the post-quantum plugin (QSMO) combines hybrid signature and hybrid encryption with the legacy signature and encryption provided by Outlook's native S/MIME layer.

### If legacy Outlook S/MIME is enabled




1. **Concatenate** both digital signatures
2. **Encrypt** with pre-quantum algorithm first
3. **Encapsulate** with post-quantum algorithm

**[If legacy Outlook S/MIME is enabled]**

4. **Sign** with pre-quantum algorithm
5. **Encrypt** with pre-quantum algorithm

**[If legacy Outlook S/MIME is enabled]**

6. **Decrypt** with pre-quantum algorithm first
7. **Verify** pre-quantum signature

8. **Decapsulate** with post-quantum algorithm first
9. **Decrypt** with pre-quantum algorithm
10. **Verify** both digital signatures to be valid

## 3.2 FUNCTIONAL TESTS AND EXCEPTION HANDLING

To assess the feasibility and effectiveness of implementing post-quantum cryptography for email transactions, the tests were tailored to verify both the functional and exception handling aspects of email usage. The primary focus was on ensuring the seamless operation of digital signature and encryption features to bolster email security through post-quantum cryptography, while minimising any adverse impact on the user experience. Additionally, exception handling mechanisms were essential to prevent the inadvertent transmission of emails to recipients lacking imported certificates, as well as to authenticate senders and detect fake or mismatched digital signatures. The scenario results are documented in Annex B.

| SCENARIOS | EXPECTED RESULTS |
|---|---|
| **FUNCTIONAL TESTS** | |
| 1 Send a signed email. | The pqc-signed email should be verified by recipient. |
| 2 Send an encrypted email. | The pqc-encrypted email should be decrypted by recipient. |
| 3 Send a signed and encrypted email. | The pqc-signed and pqc-encrypted email should be verified and decrypted by recipient. |
| 4 Send an encrypted email with attachments. | The pqc-encrypted email with attachments should be decrypted by recipient. |
| 5 Send an encrypted email to several recipients. | The pqc-encrypted emails should be decrypted by all recipients. |
| 6 Send an encrypted email with attachments to several recipients. | The pqc-encrypted emails with attachments should be decrypted by all recipients. |
| **EXCEPTION HANDLING TESTS** | |
| 7 Send an encrypted email to a recipient without certificate. | Email plugin intercepts and informs the sender that the recipient certificate is missing. |
| 8 Send a fake signed email | Recipient cannot verify pqc-signed sender who uses a P12 certificate other than his own. |

Figure 5 | Scenarios and Expected Results





# FINDINGS & DISCUSSION

## Challenges and insights in a near-standard environment

4

### 4.1. LESSONS LEARNED

#### Observation

The longer key lengths of CRYSTALS-Dilithium and CRYSTALS-Kyber may not have a significant impact on low-transaction applications, such as email usage. This is advantageous for securing simple end-user applications. However, in the case of financial transactions, which may involve a higher volume of activities compared to reading emails, it is important to explore whether longer key lengths in cryptography have a consequential impact. Further research is warranted to assess the potential downstream effects of longer key lengths on cryptographic security in high-transaction financial applications.

#### Challenges

The experimentation presented several challenges. Firstly, there were issues with the mail server processing a new email format. Existing email plugins, policies, or anti-malware systems might modify message headers or block emails due to unrecognised formats. Some systems may even issue warnings to recipients about unknown senders. These issues stemmed from the hybridised S/MIME content type and attachment extensions, leading to downstream complications.

Secondly, the Outlook application inherently recognises digital signatures, which posed a challenge as the PQC email plugin couldn't process

hybrid digital signatures ahead of Outlook. However, in sign-and-encrypt operations, the PQC email plugin is the sole entity capable of decrypting and subsequently verifying the digital signature. Hence, this is not a problem for the latter.

### Insights

To establish resilient email communication channels, organisations should consider the following steps:

- Adopting quantum-safe cryptography: Utilise quantum-safe cryptographic algorithms for key exchange, digital signatures, and encryption to ensure that the entire email communication process is resistant to quantum attacks.

- Addressing new email formats: Introducing a new email format can potentially disrupt email communication channels. This necessitates thorough testing to prevent undue disruption.

- Understanding your application behaviour: While we have addressed Outlook's automatic processing of digital signatures, it is crucial to recognise that other mail clients or applications may behave differently. Therefore, any hybridisation efforts should involve careful investigation into application behaviour.

By taking these measures, organisations can work towards establishing a robust and consistent approach to quantum-safe email communication.

## 4.2. FUTURE WORK

### Investigating interoperability

Building on the work of this experimentation, another approach can be taken to enhance the interoperability objectives. In this modified scenario, BDF will continue to use CryptoNext's QSMO plugin, while MAS will test another local email plugin or client to replicate the existing functionality (see 3.1).

This approach aims to demonstrate that, given the exchange of necessary certificates, the plugin or software interface leveraging post-quantum cryptography libraries can remain agnostic.

### Expanding into financial applications

Expanding beyond email transactions, the broader objective is to investigate using post-quantum cryptography for critical financial transactions. For instance, this could extend to cross-border PQC security over payment networks.

The first point to consider is whether cross-border PQC security over payment networks is viable. This involves evaluating the latency and efficacy of traditional and PQC algorithms when used together.

Additionally, the level of cross-border cooperation and coordination required between industry, central banks, and payment network actors need to be examined. This includes understanding the necessary operating parameters, timing, governance, and other factors that would facilitate the successful integration of PQC security measures into the existing payment networks.

Finally, it is crucial to identify any limitations of existing technology solutions both in terms of technical and operational aspects. This assessment will assist industry stakeholders in identifying and addressing any shortcomings when integrating PQC-based solutions and related hardware into existing systems.



QUANTUM-SAFE EXPERIMENT REPORT - 2024

# CONCLUSION

# 5

## An initial collaboration that paves the way for future partnerships

The collaborative PQC experimentation between BDF and MAS marks a significant milestone in our collective efforts to future-proof our communication systems against emerging quantum threats. Throughout this initiative, we successfully exchanged signed, encrypted, and both signed-and-encrypted emails. This achievement demonstrates our ability to integrate PQC algorithms within BDF's standard environment and modern architectures, including MAS' cloud provider, ensuring that these technologies are viable for practical, real-world applications.

**This achievement demonstrates our ability to integrate PQC algorithms within BDF's standard environment and modern architectures, including MAS' cloud provider, ensuring that these technologies are viable for practical, real-world applications.**

Additionally, in the event of a sudden breach in legacy algorithms, BDF and MAS have demonstrated the capabilities to swiftly implement a hybrid PQC messaging system. This deployment requires minimal modifications to the existing infrastructure, with only a plugin needed for integration.

Our experimentation also highlighted the need to define our own hybridisation choices. Specifically, the absence of draft standards for PQC hybrid S/MIME underscores the need for proactive development and standardisation efforts from regulatory and standardisation organisations.

Moreover, this project fostered a strong partnership between BDF and MAS, laying the groundwork for future collaborations in PQC and other areas of cybersecurity. The algorithms we tested and implemented for email encryption and signature are versatile and can be applied to other critical settings, such as secure payment systems.

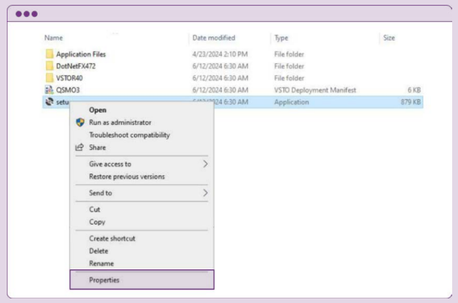
In conclusion, our successful experimentation not only advances our understanding and application of PQC but also sets a precedent for future initiatives. By pioneering these efforts, BDF and MAS are at the forefront of securing digital communications in the quantum era, ensuring the continued trust and resilience of our information systems.

# ANNEXES

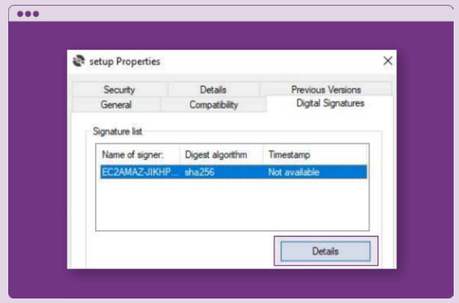
# POST-QUANTUM CRYPTO-GRAPHY



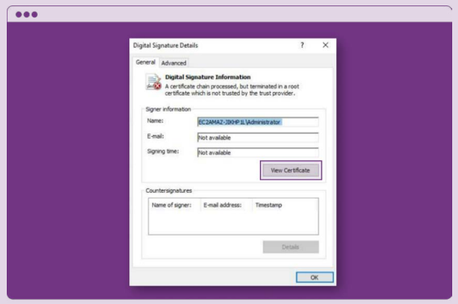
## ANNEX A | INSTALLATION STEPS [1/4]



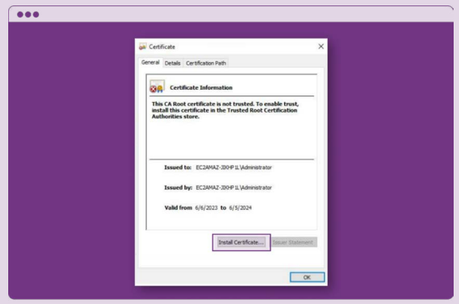

1 Open installation folder. Right click on setup file. Click on Properties.



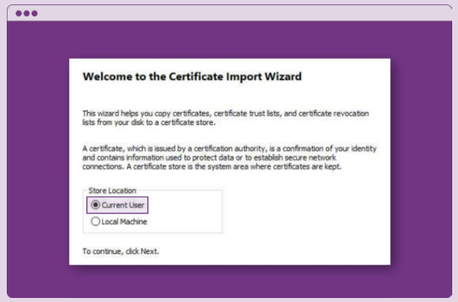

2 Go to Digital Signatures tab. Select the signer and click Details.



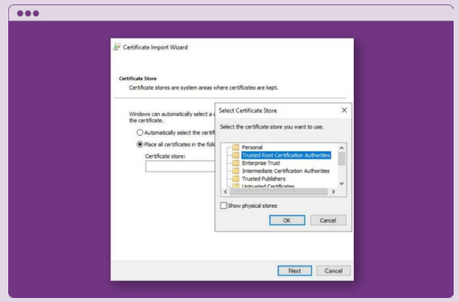

3 Click View Certificate.




4 Click Install Certificate.

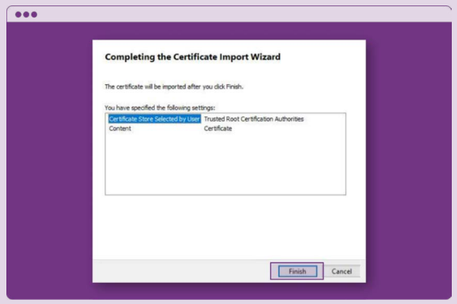



5 Select Current User.

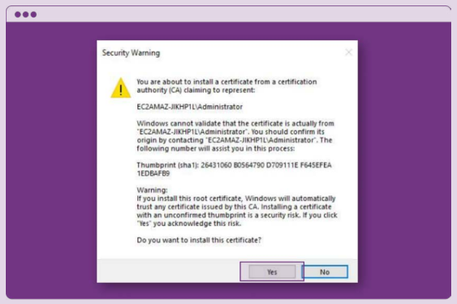



6 Place all certificates under Trusted Root Certification Authorities.

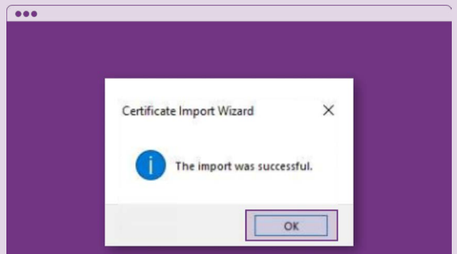
## ANNEX A | INSTALLATION STEPS [2/4]



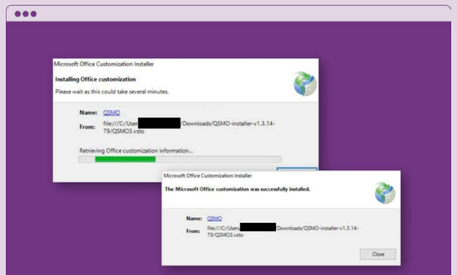

7 Click Finish.



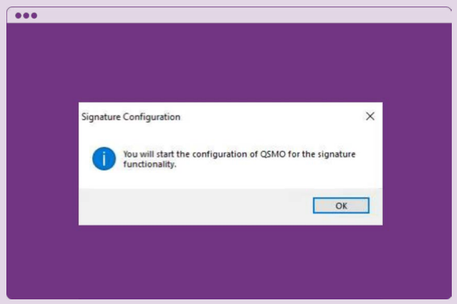

8 Click Yes.



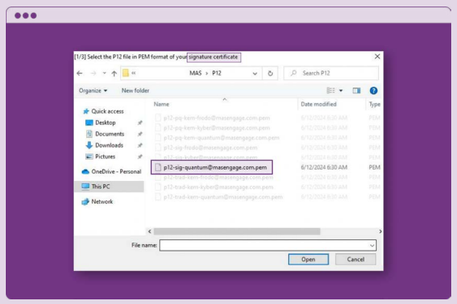

9 Click Ok.




10 Go back to the installation folder. Double click on setup file to install.




11 Open Outlook. QSMO configuration will begin. As an example, the following will walk through the setup for user quantum@masengage.com.

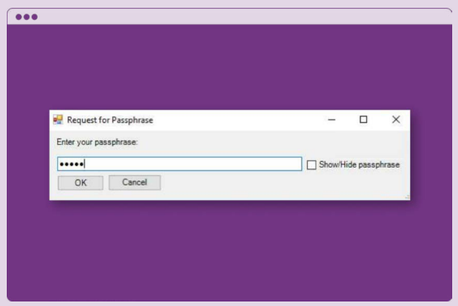



12 Import PKCS#12 signature certificate for user quantum@masengage.com.



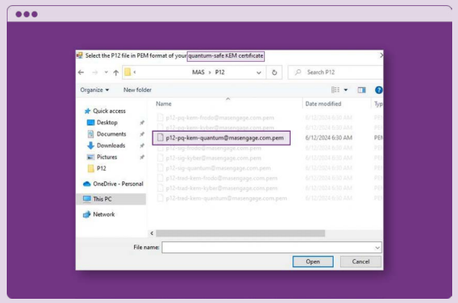


## ANNEX A | INSTALLATION STEPS [3/4]

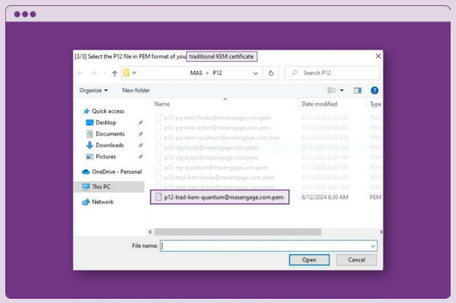



13 Enter the passphrase.

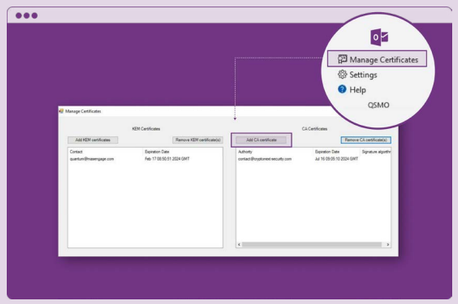

14 Click Ok.



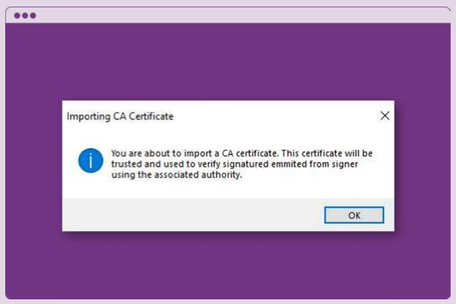

15 Import PKCS#12 post-quantum KEM certificate for user quantum@masengage.com.




16 Import PKCS#12 traditional KEM certificate for user quantum@masengage.com.

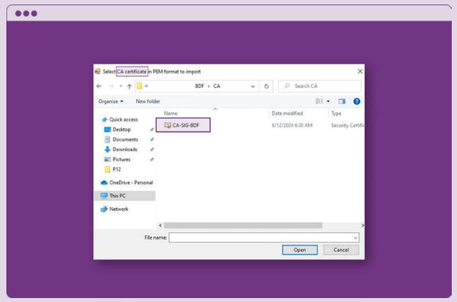



17 On top right of Outlook, find QSMO plugin and click Manage Certificates, follow by Add CA Certificate.

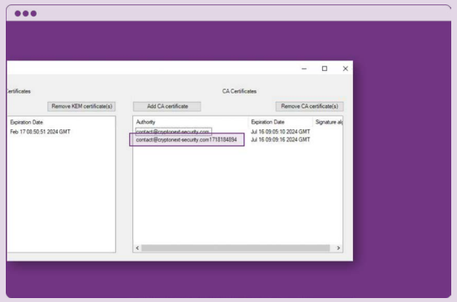



18 Click Ok to import CA certificate.

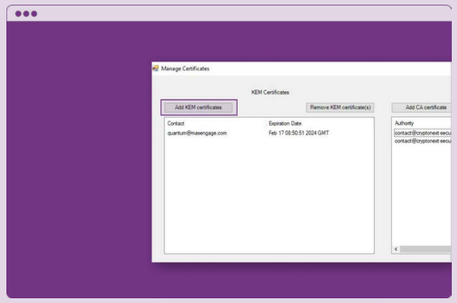
## ANNEX A | INSTALLATION STEPS [4/4]



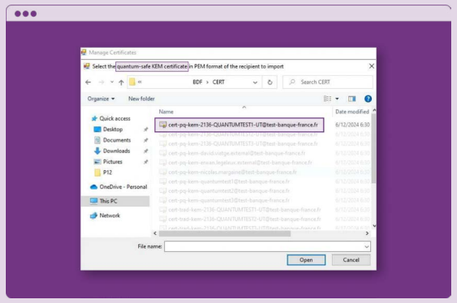
19 Open CA folder and select CA certificate.



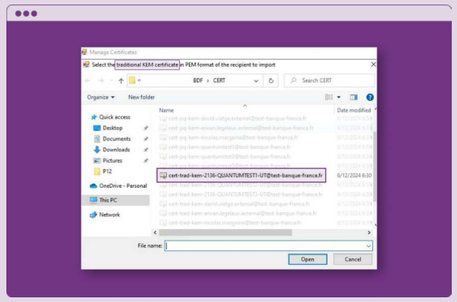
20 The CA certificate appears in QSMO plugin.



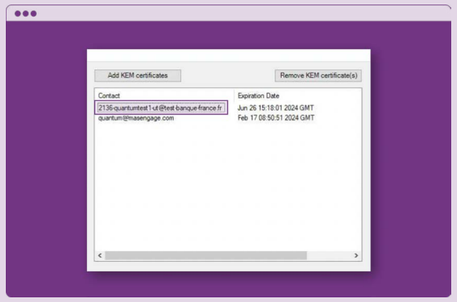
21 Next, on the same window, click Add KEM certificate.



22 Import post-quantum KEM certificate for user 2136-QUANTUMTEST1-UT@test-banque-france.fr.



23 Import traditional KEM certificate for user 2136-QUANTUMTEST1-UT@test-banque-france.fr.



24 The certificates for user 2136-QUANTUMTEST1-UT@test-banque-france.fr are added.



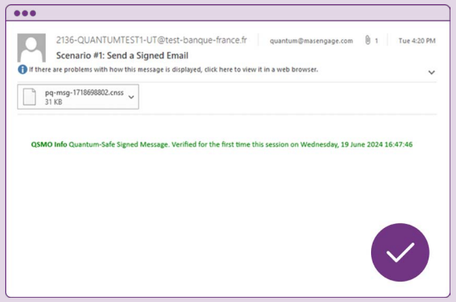


## ANNEX B | FUNCTIONAL TESTS AND EXCEPTION HANDLING RESULTS [1/2]

### 1. Functional tests

Scenario #1

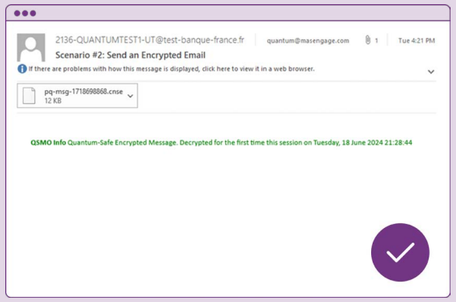
**Send a signed email.**




**Expected result:**
The pqc-signed email should be verified by recipient.

Scenario #2

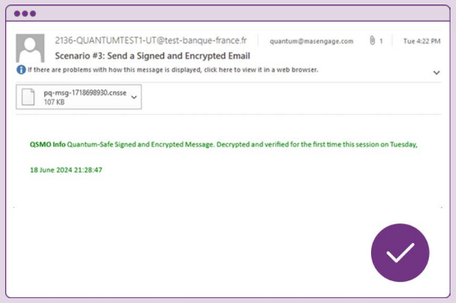
**Send an encrypted email.**




**Expected result:**
The pqc-encrypted email should be decrypted by recipient.

Scenario #3

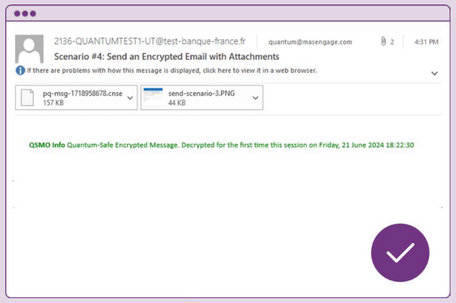
**Send a signed and encrypted email.**




**Expected result:**
The pqc signed and encrypted email should be verified and decrypted by recipient.

Scenario #4

**Send an encrypted email with attachments.**

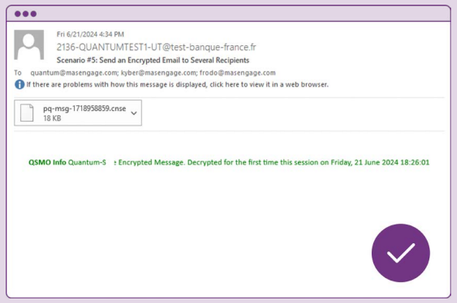



**Expected result:**
The pqc-encrypted email with attachments should be decrypted by recipient.

## ANNEX B | FUNCTIONAL TESTS AND EXCEPTION HANDLING RESULTS [2/2]

Scenario #5

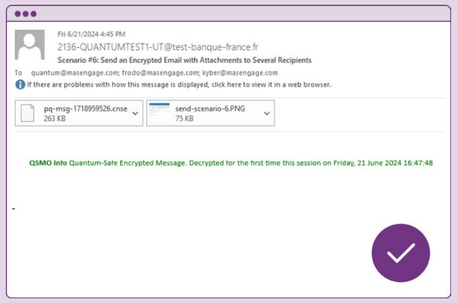
**Send an encrypted email to several recipients.**




**Expected result:**
The pqc-encrypted email should be decrypted by all recipients.

Scenario #6

**Send an encrypted email with attachments to several recipients.**

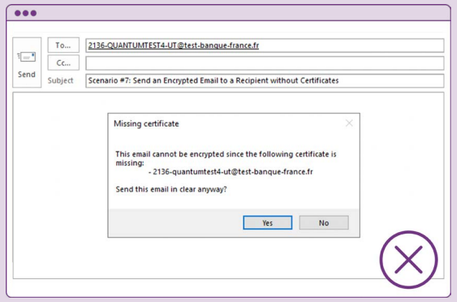



**Expected result:**
The pqc-encrypted email with attachments should be decrypted by all recipients.

### 2. Exception handling tests

Scenario #7

**Send an encrypted email to a recipient without certificates.**




**Expected result:**
Email plugin intercepts and informs the sender that the recipient certificate is missing.

Scenario #8

**Generate a fake signed email.**


**Expected result:**
The recipient cannot verify pqc-signed sender who uses P12 certificate other than his own.



BANQUE DE FRANCE EUROSYSTÈME

MAS Monetary Authority of Singapore

# Securing digital communications between the Banque de France & the Monetary Authority of Singapore

Quantum-safe experiment report, November, 2024

**Authors**

**Nicolas Margaine**
Cryptography Project Manager, Banque de France

& Banque de France team

**Edwin Goh**
Deputy Director, Monetary Authority of Singapore

& Monetary Authority of Singapore team

**Project Sponsors**

**Damien Pang**
Deputy Chief FinTech Officer and Head, Monetary Authority of Singapore

**Claudean Zheng**
Chief Information Security Officer, Monetary Authority of Singapore

**My Phuong Dulman**
Head of Digital, le Lab, Banque de France



Monetary Authority
of Singapore