Quantum Key Distribution
Proof-of-Concept Sandbox
for the Financial Sector

Post-Implementation Report

An Industry collaboration

Supported by:

Monetary Authority of Singapore

Participating banks:

DBS HSBC OCBC UOB

Participating technology partners:

SPEQTRAL sptel Reliability with an Edge

Contents

1. Foreword

The dawn of the quantum era brings not just new promises and opportunities but also risks and challenges. Quantum computing is poised to greatly enhance computations to potentially revolutionise industries—but alongside this opportunity comes a real threat to our current cryptographic systems. As the world becomes increasingly interconnected and reliant on digital technologies, protecting our sensitive data in the digital space has never been more critical.

This experiment represents a useful step towards a quantum-safe financial sector. By collaborating with leading banks and quantum key distribution (QKD) providers, we are studying and testing prospective cybersecurity solutions that can help to safeguard critical financial systems and data against the emerging quantum threats.

This initiative not only demonstrates our commitment to technological advancement but also exemplifies the culture of collaboration between the public and private sectors. By pooling our resources and expertise, we are able to accelerate our understanding of various quantum-safe solutions, one of which is QKD.

As we embark on this exciting endeavour, we invite you to join us in shaping the future of secure digital communications. Together, we can build a quantum-safe financial ecosystem that safeguards our sensitive data and ensures the integrity of our transactions.

Vincent Loy

Assistant Managing Director (Technology)
and Chief Technology Officer
Monetary Authority of Singapore

2. Executive Summary

The financial sector faces a critical threat from quantum computing that could in the coming years render today's cryptographic systems vulnerable to attack. In anticipation of the future threat posed by quantum-powered decryption, MAS:

- Published an advisory to financial institutions (FIs) on addressing cybersecurity risks associated with quantum computing in February 2024. The advisory highlights measures that FIs should consider as part of their quantum transition efforts;[1] and
- Conducted trials to study the viability of quantum-safe solutions for adoption in financial services.
  - In November 2024, MAS and Banque de France announced the completion of a milestone experiment using Post-Quantum Cryptography (PQC) to secure international electronic communications.[2]
  - In August 2024, MAS, DBS, HSBC, OCBC, UOB, SPTel, and SpeQtral signed a Memorandum of Understanding (MoU) to conduct a proof-of-concept (PoC) sandbox on QKD in financial services. The initiative is designed to test QKD's effectiveness in safeguarding financial communications and boost the sector's overall quantum readiness.

The PoC allowed participating organisations to experiment with the use of QKD to securely transfer simulated test financial data. The QKD solution used in the sandbox, jointly provided by SPTel and SpeQtral, enabled MAS and the participating FIs to protect these data using encryption keys shared over a quantum-safe channel. The PoC allowed MAS and the participating FIs to collaborate and deepen their understanding of QKD. The sandbox also provided insights into the benefits and limitations of QKD solutions, that will guide MAS and the participating FIs to make informed decisions on quantum-safe strategies and bolster our cyber resilience against quantum threats.

The key findings from the PoC included:

- Potential use cases of QKD in financial services. QKD has the potential to strengthen the security of communication networks used by FIs to transmit sensitive financial information. Its application can include securing connections between data centres and the FIs.
- Need for QKD providers and the telecommunications sector to continue strengthening QKD security assurance, such as establishing comprehensive standards for tamper-resistant, auditable trusted nodes with multi-layer security measures.
- For QKD to be widely adopted in the financial sector, it needs to be more tightly integrated globally into diverse IT environments with interoperability across different QKD providers.

While QKD shows strong potential, its successful deployment must overcome barriers such as cost, complexity, scalability and the security in the architecture of trusted nodes. Beyond the technical takeaways, the sandbox also underscored the importance of strong senior management support to prioritise quantum-safe initiatives within cybersecurity and broader technology budgets as well as research and development allocations. It also highlighted the need to equip staff with technical competencies to effectively evaluate and appropriately implement QKD solutions in anticipation of quantum security threats.

Moving forward, continued collaboration between FIs, QKD providers, the telecommunications sector and regulators will be key to establishing robust standards, scalable frameworks, and seamless interoperability. This PoC represents a step towards a quantum-safe financial sector.

[1] MAS. (Feb 2024). MAS/TCRS/2024/01: Advisory on Addressing the Cybersecurity Risks Associated with Quantum (see https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum).
[2] MAS, BdF. (Nov 2024). (see https://www.mas.gov.sg/news/media-releases/2024/bdf-and-mas-conduct-groundbreaking-post-quantum-cryptography-experiment).

3. Introduction

3.1
The Quantum Threat to Cryptography

Advances in quantum computing could potentially undermine the security of current cryptographic systems, due to the threats posed by quantum algorithms like Shor's algorithm and Grover's algorithm.

Shor's algorithm can break commonly used asymmetric-key cryptography, such as Rivest-Shamir-Adleman (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH). Grover's algorithm could also threaten symmetric-key encryption, like the Advanced Encryption Standard (AES), albeit to a much lesser extent.

At this point, the capabilities of the latest quantum computers are still limited, and not yet able to run Shor's algorithm to an extent that would effectively crack the quantum-vulnerable cryptography used in modern-day encryption. However, the threat will eventually materialise when quantum computing technology advances further, and cryptographically relevant quantum computers (CRQCs) become available.[3]

Governments are moving to mitigate the quantum threat. The US' National Institute of Standards and Technology (NIST) began developing PQC standards in 2016 and published the first set in August 2024. PQC relies on "one-way trapdoor" functions that are secure against Shor's and Grover's algorithms, enabling quantum-safe key establishment, encryption, and digital signatures. Agencies like the US National Security Agency (NSA), NIST, the European Union (EU) Commission, and the UK's National Cyber Security Centre (NCSC) recommend beginning PQC migration planning now.[7,8,9,10]

3.2
Securing Communications with Quantum Key Distribution

While PQC relies on computational complexity and mathematical hardness, it is not the only solution available in the quantum-safe toolkit. Organisations can implement quantum-safe security through a layered strategy that combines the mathematical hardness of PQC with the physics-based approach of using QKD for key establishment. QKD uses the principles of quantum physics to enable two parties to establish secret encryption keys securely through a quantum communication channel with intrinsic tamper-evident capabilities.

The BB84 protocol was introduced by researchers Charles Bennett and Gilles Brassard in 1984 as the first QKD protocol and laid the foundational framework for QKD. QKD achieves security by relying on the fundamental principles of quantum mechanics rather than the hardness of certain mathematical problems.[11] Because QKD systems use quantum properties of light particles to generate encryption keys, any attempt to intercept or copy the key will alter the photons' properties.

If an eavesdropper tries to tap the signal, the QKD system detects the interference and alerts the users that the encryption key exchanged may be compromised. That information is then discarded, ensuring that only secure information is used for the keys. Once verified, QKD-derived keys can then be used for encryption and decryption with symmetric-key algorithms, such as AES 256 (see Fig. 1).

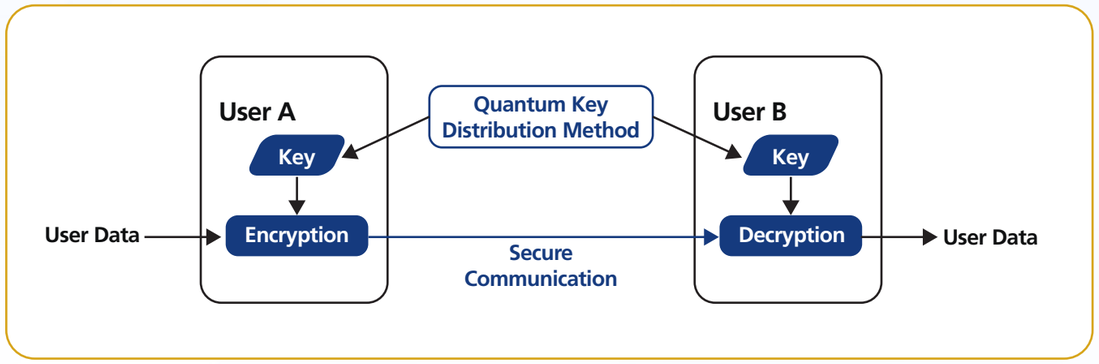

Figure 1: QKD: Overview and Encryption/decryption

[3] CRQC refers to a quantum computer that can efficiently break real world cryptographic systems.
[4] NIST. (Apr 2016). Report on Post-Quantum Cryptography. (see https://www.nist.gov/publications/report-post-quantum-cryptography).
[5] The first four NIST PQC algorithms are CRYSTALS-Kyber/ML-KEM for public key encryption, and CRYSTALS-Dilithium/ML-DSA, FALCON/FN-DSA, and SPHINCS+/SLH-DSA for digital signatures. Beyond the published standards, NIST continues to standardise new PQC algorithms. Other jurisdictions such as France and Germany have also identified additional PQC algorithms, such as FrodoKEM and Classic McEliece.
[6] A one-way trapdoor function is a mathematical operation that is easy to compute in one direction but computationally infeasible to reverse without specific secret information (i.e. the trapdoor).
[7] NSA. (Sep 2022). NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems. (see https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/).
[8] NIST. (Nov 2024). IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards. (see https://csrc.nist.gov/pubs/ir/8547/ipd).
[9] EU Commission. (Jun 2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. (see https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography).
[10] NCSC. (Mar 2025). Timelines for Migration to Post-quantum Cryptography. (see https://www.ncsc.gov.uk/guidance/pqc-migration-timelines).
[11] Bennett, C. H.; Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India. Vol. 1. New York: IEEE. pp. 175–179. (see https://arxiv.org/abs/2003.06557.)

4. Setting up the QKD Proof-of-Concept Sandbox

4.1
QKD Framework and Architecture

QKD leverages the principles of quantum physics to create identical copies of secret keys at two endpoints, which can then be used as symmetric keys. It can be implemented through optical fibre or free-space channels such as satellites. This PoC used fibre-based QKD as part of the Infocomm Media Development Authority's (IMDA's) National Quantum-Safe Network Plus (NQSN+) infrastructure.[12] This PoC also adopted a QKD framework aligned with relevant standards, recommendations and specifications from the European Telecommunications Standards Institute (ETSI), IMDA, International Organization for Standardization (ISO) and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), structured around three key layers (see Fig. 2):

a. **Secure Application Entity (SAE) Layer** – where encryption or cryptographic applications consume the quantum-safe keys, and utilise them for applications such as securing data in transit or at rest. This is the layer that utilises keys retrieved from the Key Management Service Layer.

b. **Key Management Service (KMS) Layer** – where QKD-derived keys are stored, relayed, and made available to the SAEs.

c. **QKD Layer** – the foundation layer where single photons are exchanged to produce quantum-safe keys based on quantum physics. There is also classical communication that takes place at this layer.

The PoC utilised a trusted-node infrastructure[13] where the security of keys that are produced, stored, relayed, and consumed are grounded in the laws of quantum physics, and are secure against any attempted deciphering attack even if the attacker has unbounded computational resources. Keys used for symmetric encryption of files transferred between MAS and participating FIs were delivered to the SAE layer in accordance with the ETSI GS QKD 014 technical reference specification.

The QKD infrastructure also utilises physical controls similar to those used in data centres to protect the QKD appliances housed in server rooms. These include two-factor authentication, requirement for external parties to be escorted, and closed-circuit television camera surveillance for access to server racks housing QKD appliances. For SPTel's QKD infrastructure used in this PoC, the trusted nodes are located in power substations that are managed by SPTel. These are officially designated as critical infrastructure and subject to protection measures such as armed guards, fencing, and physical intrusion detection system. Additionally, the server rooms housing QKD appliances are protected with environmental control systems such as fire suppression, and temperature and humidity control.

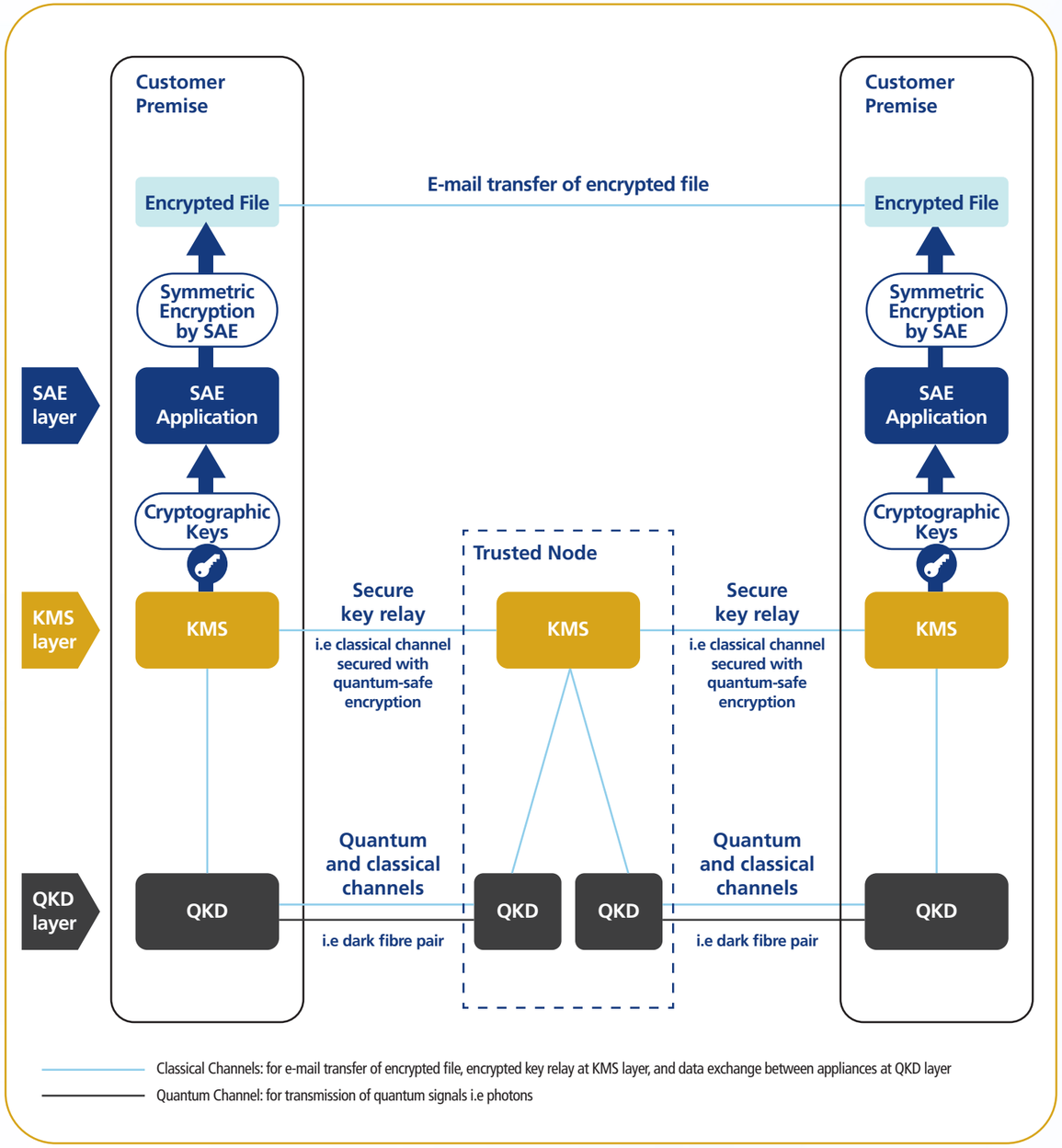

Figure 2: SAE, KMS, and QKD layers in the PoC sandbox

[12] IMDA's NQSN+ will support network operators to deploy quantum-safe networks nationwide (see https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/national-quantum-safe-network-plus).
[13] See next section 4.2, and Annex B for details on trusted-node infrastructure.

4.2
Trusted-Node Infrastructure

In multi-site or inter-organisational setups, a QKD network (QKDN) can use trusted nodes as secure relays to scale across greater distances and connect multiple sites securely. This PoC demonstrated such connectivity between MAS and participating FIs via trusted nodes on the NQSN+ network (see Annex B for details on trusted nodes).

The PoC was conducted in two windows, with three sites involved at a time. Window one (Sep–Nov 2024) involved MAS, DBS and OCBC, while window two (Jan–Mar 2025) involved MAS, HSBC and UOB (see Fig. 3).

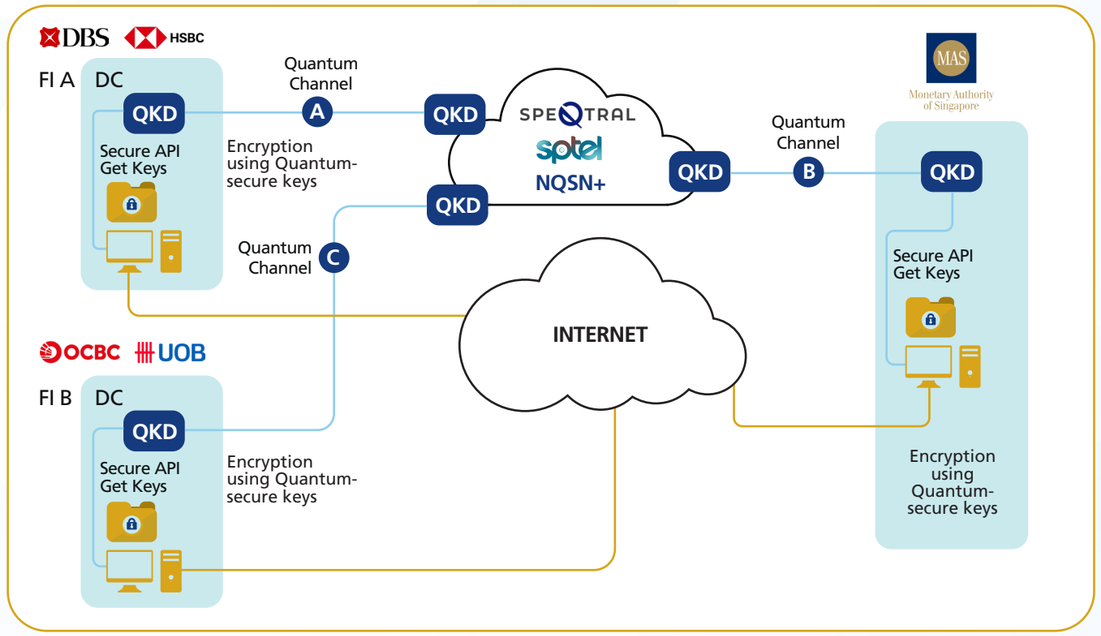

Figure 3: QKD connections between MAS and FIs via NQSN+ trusted node

4.3
Customer Premise Infrastructure

Deployment at the QKD customer's site involves a QKD stack comprising the QKD equipment, key management server, and network switches for connectivity. The QKD equipment handles key generation, while the key management server manages key relay, secure storage, and the delivery of keys to applications or client appliances (see Fig. 4).

For this PoC, MAS and the participating FIs set up sandbox environments isolated from their production networks. Each participant:

a. Housed the QKD stack in a secure, on-premise data centre with appropriate physical safeguards.

b. Allocated at least seven rack units (RUs), a power supply of no more than 1kW and two fibre links to support the QKD stack.

c. Deployed the QKD stack within the same rack as the rest of the system for simplicity and containment.

d. Set up a test workstation equipped with user application software that is connected to the QKD stack KMS using the ETSI GS QKD 014 ethernet-based representational state transfer (REST) application programming interface (API) to obtain quantum-safe keys for cryptographic applications (see Fig. 5).

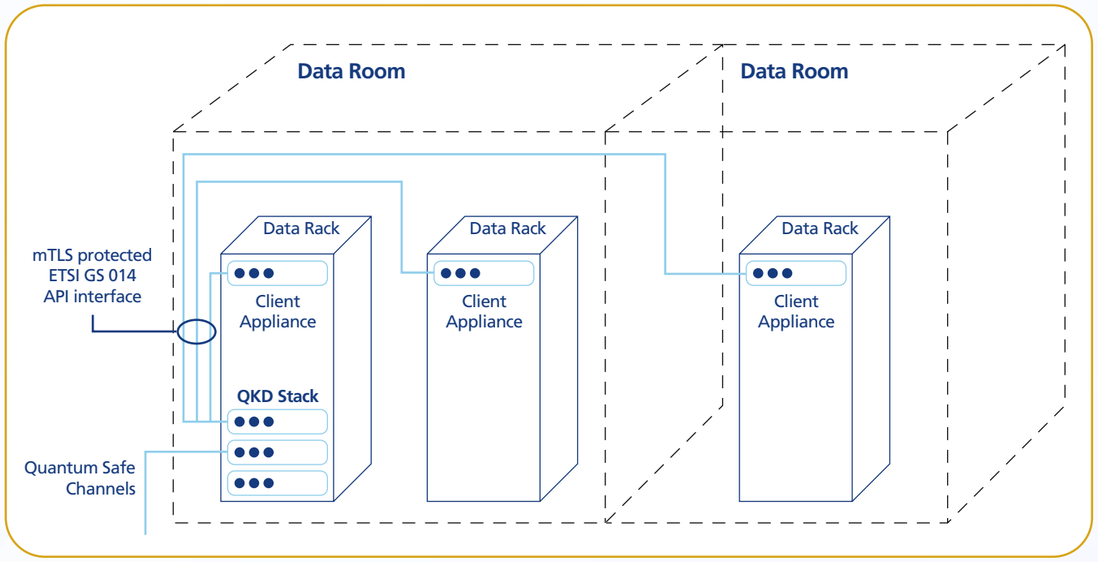

Figure 4: PoC setup at each location - QKD stack within the same rack

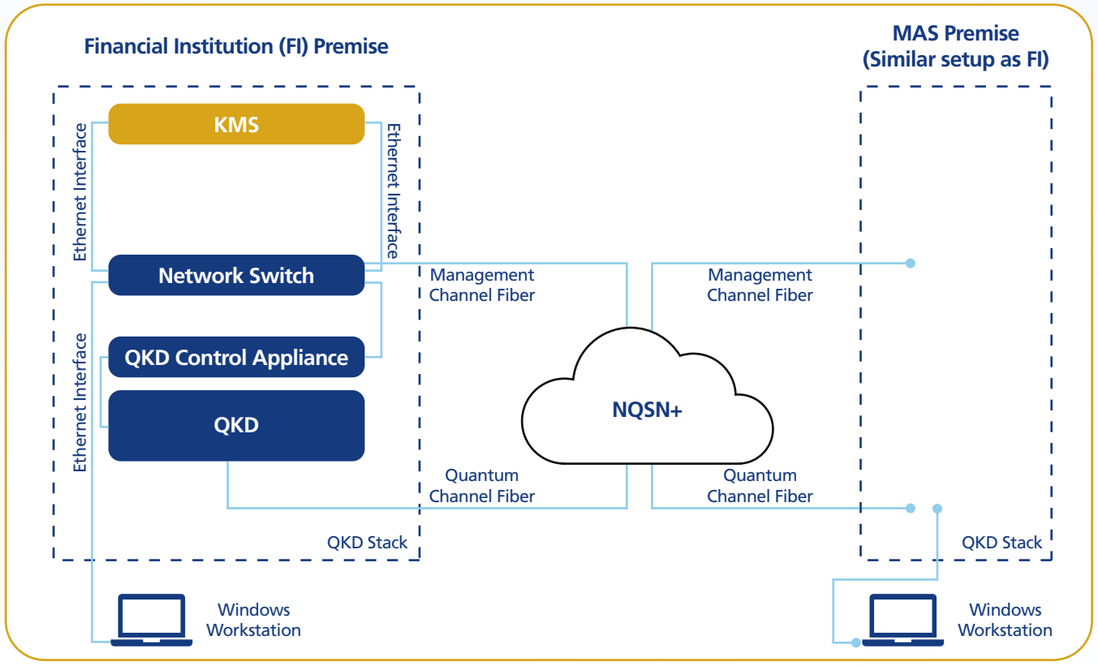

Figure 5: Illustration of QKD stack at MAS and FIs

4.4
Secure Application Entity: Custom File Encryption Tool

Secure Application Entities (SAEs) in a QKDN setup request keys from the KMS appliance to perform cryptographic applications such as encryption and decryption. In a QKD setup, these SAEs are typically network security appliances supporting data in-transit scenarios (see Annex B for examples). Some may also include machines or appliances integrated with Hardware Security Modules (HSMs), enabling support for applications such as databases, key vaults, or commercial cloud services.

For this PoC, one of the use cases is to secure the exchange of electronic files (containing settlement instructions) between MAS and participating FIs for processing in the MAS Electronic Payment System (MEPS+), which is Singapore's real-time gross settlement system (RTGS). Specifically, this is performed during the contingency scenario where potential alternative electronic channels to the main channel need to be activated while ensuring cybersecurity resilience.[14] A software-based front-end custom file encryption tool was used to function as the SAE to support testing (see Fig. 6 and Fig. 7). The tool was containerised as a docker image and deployed on a Windows workstation via Windows Subsystem for Linux (WSL). It enabled encryption and decryption of test files or folders using keys retrieved through API calls from the QKD KMS. Each encrypted file embedded the key ID as metadata, allowing the tool to identify and fetch the corresponding key from the QKD KMS for decryption (see Annex B Fig. B for further details on key consumption).

The PoC setup also incorporated a software development environment that facilitated API testing, troubleshooting, and automation to facilitate advanced testing (e.g bulk key retrieval, and timed key requests to simulate load testing).

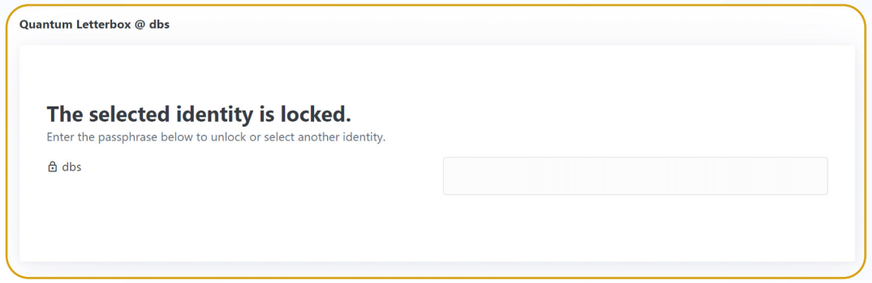

Figure 6: Interface for users to access the SAE file encryption tool

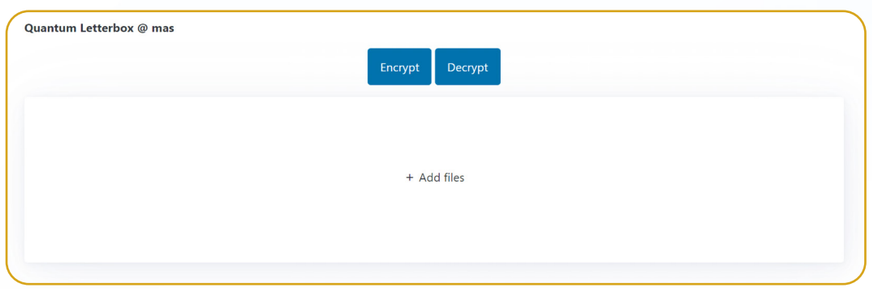

Figure 7: Interface for encryption and decryption of test files

[14] https://www.mas.gov.sg/regulation/payments/meps

5. Testing Quantum-Safe Communications

5.1
Identifying Core Test Cases

The PoC explored the performance of the QKDN through three categories of test cases during the exchange of MEPS+ files between MAS and the participating organisations:

- **Operational** – to observe how the QKDN performs during key generation, and encryption and decryption of the transmitted electronic MEPS+ files.
- **Security** – to verify the system's ability to detect and reject incorrect credentials or configurations.
- **Resilience** – to assess how the system responds to and sustains operations during physical network disruptions.

These tests provided practical insights into QKD integration and policy development.

5.1.1
Operation-focused Tests

a. **Monitoring Metrics** – Participants tracked Quantum Bit Error Rate (QBER) and Secure Key Rate (SKR) via a dashboard to gauge system health and performance of connections between end points (be it FI or MAS) to the trusted node.

b. **Key Retrieval & ID Association** – Verified that keys could be retrieved and correctly identified via ETSI GS QKD 014-compliant interfaces, using tools like curl.

c. **File Encryption/Decryption** – Tested single and bulk file encryption. Real-time key usage and refill metrics were visible, providing end-to-end transparency.

5.1.2
Security-focused Tests

Three key tests were designed to assess how well the system handles authentication errors, resists misuse, and mitigates attempted eavesdropping attacks:

a. Key Retrieval Errors

These tests confirmed that the KMS blocks unauthorised attempts and logs them for review:

- **Wrong IP Address** – The KMS rejected requests from unauthorised IPs, showing effective enforcement of network policies.
- **Invalid Certificates** – The system denied access when incorrect certificates were used during mutually authenticated Transport Layer Security, and recorded the attempts for admin alerts.

b. Decryption Errors

These tested the system's ability to reject misuse during decryption:

- **Tampered Metadata** – Decryption requests using wrong or altered metadata (e.g. key ID, SAE ID) were correctly blocked, demonstrating protection against misconfiguration or tampering.

c. Eavesdropping Attack Simulation

The practical execution of an eavesdropping attack against a QKD system presents significant technical hurdles. As such, the PoC included a simulated attempted eavesdropping attack on the QKD system by using optical attenuators to remove signal photons in the QKD connection, simulating

interception of the photons by an adversary who is attempting an eavesdropping attack (see Fig .8). The fundamental principles of quantum mechanics ensure that even perfectly executed attacks cannot obtain key information, as any interception attempts are revealed during key verification through increased error rates, allowing compromised keys to be discarded.

During the PoC, participants were able to observe the theoretical basis for QKD's security properties by observing key metric changes in a QKD system that was being subjected to an attempted eavesdropping attack, and to observe how the system responds.

For the attack simulation, the QKD system was initially operated normally with users being able to view metrics on QKD system performance such as the SKR. Optical attenuation was then added to the transmission fibre, removing photons transmitted between the QKD systems and simulating an eavesdropper's actions. It was observed that the SKR decreased during the simulated eavesdropping attack, indicating that photon states that could be possibly known to an eavesdropper were not being used to generate keys.

The QKD system design ensures that all keys produced remain secure and unknown to any third party even during an attempted eavesdropping attack. The core functionality of a QKD system, which achieves security by relying on the principles of quantum mechanics, is that any keys produced by the QKD system are always secure.

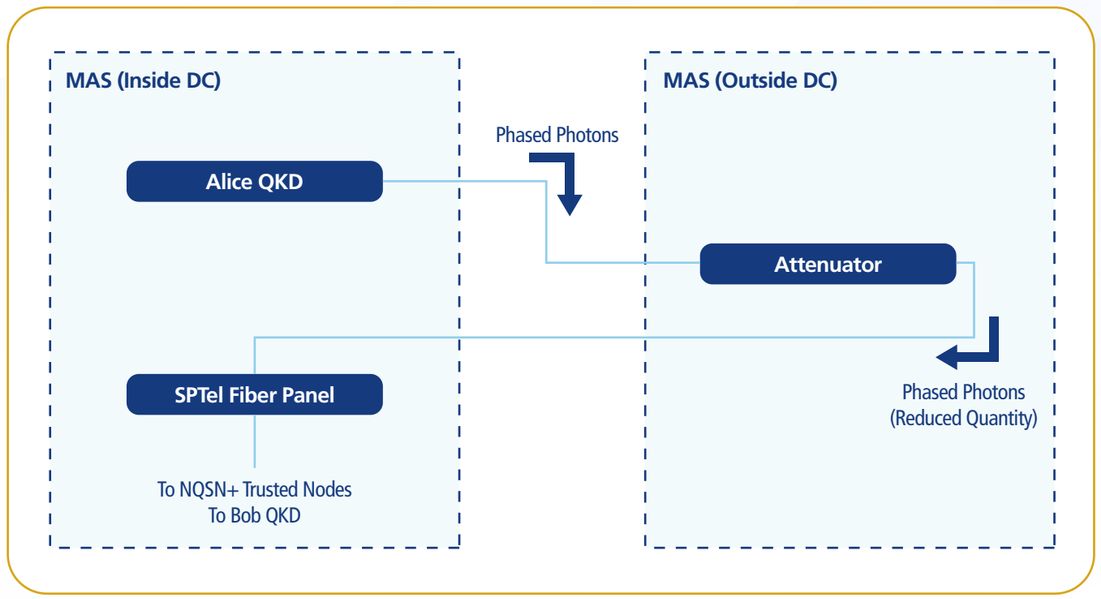

Figure 8: Simulated eavesdropping attack on PoC QKD setup using an attenuator

5.1.3
Resiliency-focused Tests

Two fibre disconnection scenarios were tested to assess the QKDN's resilience under physical network disruptions:

a. **Fibre Disconnection and Recovery of Operations:**
   This test looked at how fibre disconnection affects key retrieval. The focus was on how well the system recovered and whether it could continue retrieving keys once reconnected.
b. **Impact Assessment of Fibre Outage on Folder Encryption:**
   Here, the system's ability to encrypt folders and retrieve key metrics during fibre downtime was tested. The goal: see if encryption could still proceed and if the system could bounce back quickly once connectivity resumed.

In both scenarios, the QKDN continued to distribute quantum-safe keys for securely encrypting and decrypting MEPS+ files shared between MAS and participating FIs over e-mail. This was because the QKDN could continue to utilise buffered keys stored in the KMS during fibre disconnection. With a configured buffer of 6.75 million AES-256 keys per day and assuming the SAE refreshes its key every second, the KMS enables secure operations to continue for up to 2.5 months — even during fibre outages. This underscores the importance of configuring buffers for uninterrupted security. See Fig. 9 for a visual summary of all core and additional test cases across the operations, security and resilience categories.

5.2
Execution of Identified Core Test Cases

Secure file transfer between MAS and participating FIs was successfully executed using the custom SAE encryption tool. Deployed at both endpoints, the tool retrieved keys from the KMS to encrypt and decrypt electronic MEPS+ files during the PoC.
(See Annex D for a detailed walkthrough of the operational test case.)

5.3
Additional Test Cases

The core tests deepened MAS and FIs' understanding of the QKDN's capabilities but also raised new questions, especially around real-world application and integration with existing systems. This led to additional test cases exploring:

a. **Advanced operational and security scenarios**, such as system behaviour under key exhaustion or decryption attempts by unintended recipients.

b. **Cryptographic integration tests**, combining QKD with existing encryption methods to assess feasibility and performance:

- **Use of QKD with OTP for File Transfer**
  Tested pairing QKD with One-Time Pad (OTP) encryption to achieve end-to-end information-theoretic security on both key distribution and encryption. The system successfully generated a continuous supply of fresh keys for OTP encryption of files up to 500MB—ideal for high-sensitivity use.
- **Use of QKD with PQC Digital Signing for File Transfer**
  Combined QKD encryption with PQC digital signatures to ensure both confidentiality and authenticity. While QKD secures data-in-transit, PQC strengthens identity verification. The hybrid setup proved effective, with signatures verified and files decrypted successfully.
- **Use of QKD with PQC to Establish a Quantum-Safe VPN Tunnel (ML-KEM, Classic McEliece)**
  Using hash-based message authentication code (HMAC) key derivation, QKD and PQC keys (ML-KEM, Classic McEliece) were merged into a hybrid key used in WireGuard[15] to form a virtual private network (VPN) encrypted tunnel. The test confirmed that combining QKD's key supply with PQC's algorithmic defence provides layered security—even if one component is compromised the system remains secure.
- **Use of QKD with AES-256 for an Automated SFTP Transfer**
  Simulated real-world secure file transfers, using a program that automated key requests, encryption, secure file transfer protocol (SFTP) upload and recipient-side decryption. The "use and forget" approach ensured secure key handling without persistent storage vulnerabilities.

(See Fig. 9 for a summary of these advanced test cases, and Annex E for detailed rationale and execution notes.)

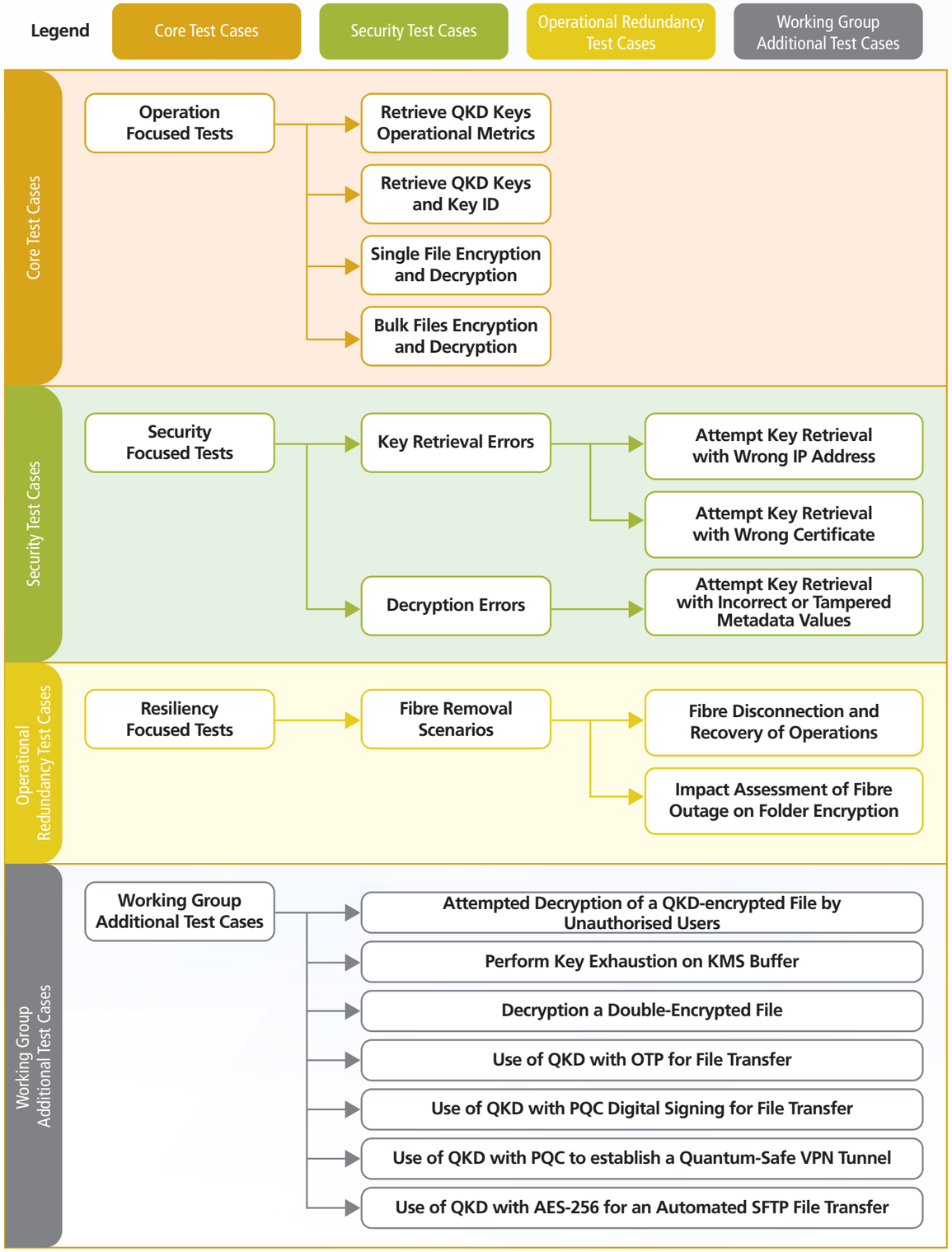

Figure 9: Overview of identified core and additional test cases for the PoC

[15] Wireguard is a general-purpose open source VPN. More information can be found at https://www.wireguard.com.

6. Key Learnings and Next Steps

6.1 Observations and Challenges During the PoC

The PoC revealed important lessons on deploying QKD in a financial services environment, especially when it comes to setup, collaboration and capability-building.

6.1.1 Importance of Resource Allocation and Stakeholder Coordination

Getting started with basic QKD tests is straightforward. But when the tests get more complex, so do the demands — from needing network architects and security specialists to ensuring seamless coordination across facilities, IT and application teams. Thoughtful planning and clear roles are essential.

Observations and Challenges	Recommendations
Resource Allocation The level of resources and expertise needed varies significantly depending on the complexity of the deployment and testing.	• Develop detailed testing, implementation, and deployment plans with clearly defined roles and responsibilities across all phases. • Implement a tiered approach towards testing, implementation, and deployment, where complexity increases step-by-step, and the right expertise is allocated at each level.
Stakeholder Coordination Multiple teams must be engaged to ensure smooth execution and integration across departments.	• Establish clear communication channels and assign responsibilities early. • Designate teams to manage various areas such as: ›› **Infrastructure** – to integrate QKD into existing network architecture ›› **Application & Cybersecurity** – to design and test real-world business use cases ›› **Governance** – to enforce controls and compliance during onboarding ›› **Facilities Management** – to ensure physical security of QKD equipment (e.g., QKD appliances)

6.1.2 Building In-House Capabilities While Tapping External Expertise

During the course of the PoC, the implementation teams from MAS and participating FIs faced a steep learning curve given their unfamiliarity with QKD technology. Staff from the IT and cybersecurity teams were required to work closely with the QKD providers to operationalise the sandbox. This highlighted the need to train and equip staff with the requisite knowledge, as well as to work closely with external experts, when implementing quantum-safe solutions.

Observations and Challenges	Recommendations
Capability and Knowledge Gaps FIs may not yet have the in-house skills to implement quantum-safe solutions.	• Build on existing IT and cybersecurity expertise to develop internal quantum capabilities—for staff training, solution evaluation and use case implementation. • Engage external experts (vendors, researchers) to fill gaps and accelerate adoption. • Hire subject matter experts to build up quantum capabilities, if resources permit. • Use PoCs and trials to build hands-on experience and uncover practical applications.

6.1.3 Strengthening Security Assurance for QKD

As FIs explore joining commercial QKD networks, confidence in QKD's security is vital. With large volumes of sensitive data at stake, FIs need assurance on trusted node security, alignment with existing controls and network resilience. QKD and telecommunications providers must step up to meet these stringent expectations.

Observations and Challenges	Recommendations
Trusted Node Security Trusted nodes must be protected against unauthorised access, as they play a pivotal role in QKDNs.	QKD providers and the telecommunications sector should: • Set tamper-resistant, auditable standards for trusted nodes. • Deploy hardware/software safeguards that trigger alerts and response to any breach attempts. • Support formal frameworks for trusted node accreditation (see Annex A).

Observations and Challenges	Recommendations
Integration with Existing Security Frameworks and Key Management In this PoC, the QKDN was kept air-gapped from live systems. But looking ahead, seamless integration with existing security frameworks is essential. That means QKD solutions must work hand-in-glove with enterprise key management processes—covering everything from access rights to governance across the full key lifecycle.	QKD providers and FIs should: • Align QKD implementations with existing security policies, especially around key lifecycle management—ensuring keys are generated, distributed, stored and retired securely and systematically. • Put in place safeguards that prevent cryptographic keys from ever being exposed in plaintext, whether at rest, in transit, or during active use.
Network Resilience QKDNs must remain stable and secure—even when things go wrong. From cyberattacks to technical faults, resilience is key to keeping performance intact and services uninterrupted.	• **Design for durability:** QKD providers and FIs should co-develop solutions with built-in failover, redundancy and high availability to safeguard mission-critical services. • **Demonstrate reliability:** Providers should show exactly how their systems bounce back from node failures or attacks—with clearly defined service level agreements that spell out uptime commitments and support protocols.

6.2 Next Steps for Scaling QKD Adoption in Financial Services

Beyond the PoC, participants also noted there could be other challenges that are crucial for future QKD implementation. These include strategically managing the complexities of implementation, and future-proofing wider adoption. QKD providers and the telecommunications sector can play a pivotal role in scaling adoption within financial services by supporting efforts to strengthen security assurance, developing comprehensive playbooks for quantum security solutions, and outlining future developments to facilitate seamless integration and adoption.

6.2.1 Strategic Support for Quantum Security Adoption

FIs require a structured path to facilitate QKD adoption, including formulating clear adoption strategies and gaining access to funding. FIs should actively monitor quantum guidance by relevant authorities and technical standard setting bodies to identify suitable uses cases for QKD based on data sensitivity and impact. QKD and telecommunications providers can support this by co-developing implementation playbooks that enable crypto-agility and align with compliance frameworks.

Potential Challenges	Recommendations
Strategy for Adoption of Quantum Security Solutions QKD adoption is complex, and FIs struggle with the lack of clear frameworks and integration paths. They need practical implementation guides, aligned regulatory compliance (e.g. MAS Technology Risk Management Guidelines, Payment Card Industry Data Security Standard) and strong cost-benefit justifications. Crypto-agility is also key—integrating QKD with PQC and evolving cryptographic standards like NIST PQC.	QKD providers and telcos should develop a playbook covering: • Step-by-step rollout guides (planning, testing, ops, training) • Compliance frameworks for encryption, key management, auditing • Cost-benefit tools: case studies, pilot validations • Crypto-agility as part of broader PQC migration efforts. This could entail demonstrating hybrid quantum security solutions that use both QKD and PQC, and how QKD solutions would be further developed to incorporate new PQC algorithms as cryptographic standards continue to evolve.
High Cost of QKD Appliances High costs of specialised gear used in QKD (e.g. photon sources, detectors, modulators) pose a barrier, especially for FIs building in-house infrastructure.	FIs can explore funding by: • Securing internal buy-in for R&D and cybersecurity budgets • Leveraging public funding (e.g. MAS' Financial Sector Technology & Innovation Scheme 3.0 Quantum Track[16]) • Collaborating in initiatives like this PoC to share costs

[16] https://www.mas.gov.sg/schemes-and-initiatives/fsti-quantum-track

6.2.2
Future-Proofing Wider Adoption of Quantum Security Solutions

This PoC underscored the need to future-proof quantum security adoption by ensuring compatibility, performance and interoperability.

For QKD to scale globally, it must integrate with current IT systems and enable secure, cross-border communications. QKD and telecommunications providers should map out future developments focused on infrastructure compatibility, interoperability across providers, and global deployment.

Potential Challenges	Recommendations
Compatibility With Existing Infrastructure QKD systems must work seamlessly within the varied IT setups of FIs, which typically include both on-premises and cloud-based infrastructure.	QKD providers and telcos could develop a framework to identify compatibility gaps and offer guidelines for smooth integration with existing IT and encryption systems.
Interoperability Considerations The PoC underscored the need for interoperability between QKD and telecommunication providers. Without standardised protocols, QKD systems from different providers may not work together.	QKD providers and telcos should co-develop interoperability strategies, guided by standards like ETSI GS QKD 020.
Future Developments for QKD QKD over optical fibres faces distance and noise limits, often requiring trusted nodes. However, it paves the way for large-scale quantum networks. Satellite-based QKD could potentially offer a scalable, low-noise solution to bridge global distances—ideal for secure, cross-border communications by FIs.	• QKD providers should develop secure cross-border solutions that address distance and regulatory challenges, enabling financial data transfer across distributed nodes. • FIs must track QKD advancements to overcome current limitations and plan for future global deployment.
Prioritisation of Quantum Security Implementation The high cost of QKD demands careful planning. FIs need to assess where it is most needed, how it should be rolled out and align deployment with budget and operational priorities.	FIs should conduct targeted assessments to: • Prioritise QKD and PQC adoption based on data sensitivity and risk impact. • Optimise spend by weighing the reuse of existing infrastructure against the need for new investments, guided by budget and operational goals.

6.3
Potential QKD Use Cases for Financial Services

Participating FIs and MAS have also identified potential QKD production use cases for securing communication within and across FIs. There are likely more immediate use cases within a single institution as opposed to across multiple FIs, since QKD supports point-to-point symmetric key distribution.

6.3.1
Securing Communications within an FI

QKD can be applied to secure communication links within an FI, including between the FIs' data centres and offices using different layers of the open systems interconnection (OSI) model.

a. **Data centre to data centre:**
   QKD can be deployed at various OSI layers to strengthen internal backbone security.
   i. **Layer 1 (Physical):**
      Use of **Dense Wavelength Division Multiplexing (DWDM)** allows QKD to run on dedicated wavelengths in optical fibres, enabling fast and secure quantum key distribution.
   ii. **Layer 2 (Data Link):**
      Integration with **media access control security (MACsec)** enables QKD to provide quantum-safe encryption keys at the Ethernet level, securing data centre traffic against tampering.
   iii. **Layer 3 (Network):**
      Combined with internet protocol security **(IPsec)**, QKD secures VPN tunnels by providing quantum-safe keys, protecting sensitive data as it moves between data centres.

b. **Data centre to office:**
   QKD can be used to encrypt sensitive data—like transaction information and customer records—travelling between central systems and office branches, ensuring secure internal operations.

6.3.2
Securing Communications across FIs and partners

QKD deployment within a single organisation allows for internally standardised protocols, while cross-organisational implementation remains challenging as industry standards for interoperability are still being developed. As QKD technology and standards mature, its symmetric key distribution capability could be extended beyond internal use to secure communication across networks of institutions.

a. **Between FIs and central banks/regulators:**
   QKD can safeguard shared platforms used by FIs and regulators, such as the MEPS+ business continuity system, ensuring regulatory data exchanges remain secure and tamper-proof.

b. **Between FIs and industry partners:**
   QKD can be paired with IPsec to protect data exchanged with external partners—such as payment processors, fintechs, or third-party vendors—by providing quantum-safe encryption keys for IP-based communication.

7. Conclusion

The financial sector stands at a critical juncture as developments in quantum computing could potentially undermine existing cryptographic methods. This report has explored QKD as a potential safeguard against these emerging threats, revealing both its promises and challenges.

QKD could potentially offer advantages in protecting financial data against quantum threats. Its security assurance stems from fundamental quantum mechanical principles, making it theoretically impossible for an eavesdropper to intercept communications undetected. This provides security against both classical and quantum computing attacks. Furthermore, the trusted node architecture in multi-site QKD deployments enhances scalability and enables long-distance secure communications, crucial for geographically dispersed financial networks. Besides its security promises, QKD adoption can also help organisations develop readiness for future and more advanced forms of quantum communications that will bring additional capabilities.

However, QKD implementation presents substantial challenges. High infrastructure costs, the need for specialised expertise, and the complexities of integration with existing systems pose significant hurdles. The security of trusted nodes emerges as a critical concern, potentially introducing vulnerabilities in QKD networks, which will be overcome through careful management and robust security protocols.

Looking ahead, FIs must develop comprehensive quantum-safe strategies that extend beyond QKD to encompass broader quantum readiness initiatives, including PQC. As the quantum landscape evolves, FIs must balance immediate security needs with long-term preparedness. This requires not only technological investments but also a focus on workforce development, risk assessment, and regulatory compliance. The integration of QKD with PQC may provide a more robust and comprehensive security solution. While QKD presents a promising path towards quantum-safe communications, its successful implementation in the financial sector demands careful planning, substantial resources, and a holistic approach to quantum security. Within this context, QKD presents an opportunity for FIs to initiate the journey towards becoming quantum-safe.

Acknowledgements

Authors

Philip Loy, Deputy Director, Technology & Cyber Risk Supervision Department, MAS

Elvina Woo, Assistant Director, Data & Technology Architecture Department, MAS

Heng Kim Chwee, Cybersecurity, Group Technology, DBS

Tan Kok Loong, Cybersecurity, Group Technology, DBS

Cheryl Tanaja, Senior Quantum Commercialisation Manager, HSBC Singapore

Alejandro R.-P. Montblanch, Quantum Communications and Networking Lead, HSBC

Sripal Jain, Emerging Technology Architect, OCBC

Ryan Zhang, Infrastructure Solutioning & Design, OCBC

Michelle Teo, SVP, Security Project Management Office, Group Technology & Operations, UOB

Omeila Fun, VP, Security Engineering, Group Technology & Operations, UOB

Alexander Dixon, Director of Quantum Projects, SpeQtral

Cyril Tan, Security Architect, SpeQtral

Heng Kwee Tong, Head, Engineering & Corporate IT, SPTel

Yong Hai Hung, AVP, IP & Transport Engineering, Engineering & Corporate IT, SPTel

Project Sponsors

Vincent Loy, Assistant Managing Director (Technology) and Chief Technology Officer, MAS

Eugene Huang, Group Chief Information Officer, DBS

Tancy Tan, Chief Operating Officer, HSBC Singapore

Praveen Raina, Head of Group Operations & Technology, OCBC

Lawrence Goh, Head of Group Technology and Operations, UOB

Lum Chune Yang, Co-Founder and Chief Executive Officer, SpeQtral

Titus Yong, Chief Executive Officer, SPTel

Annex A: Developments in QKD Technology

Quantum Key Distribution Accreditation and Standards

Globally, efforts are underway to establish accreditation and testing frameworks for QKD systems. Key milestones include:

- Publication of QKD standards by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)[17]
- South Korea's national framework for QKD testing and verification[18]
- Recognition of the European Telecommunications Standards Institute (ETSI) General Specification QKD 016 Common Criteria Protection Profile by Germany's Federal Office for Information Security (BSI)[19]

In the EU, the **EuroQCI initiative** and the **NOSTRADAMUS project**[20] are putting in place QKD testing infrastructure, while the UK's **QAssure project consortium**[21] is developing QKD security assurance schemes.

Beyond accreditation, standardisation work continues through ETSI's **Industry Specification Group (ISG) on QKD**[22] , and the **ITU-T** (International Telecommunication Union's standardisation arm)[23], focusing on interoperability and future network integration.

Ongoing Deployments of Quantum Key Distribution Systems

Today, QKD systems are commercially available from over 20 companies worldwide. Typical deployments cover up to 150 km without trusted nodes[24], with key exchange rates available up to 1 Mbps reaching 300 Kbps at 50 km. Ongoing research continues to push these limits, with new types of QKD systems demonstrated over distances of over to 1000 km[25] and key rates up to 100 Mbps in lab settings.[26]

There is growing momentum around combining QKD with PQC, through trials and PoCs, and QKD providers[27] to create robust, integrated quantum-safe security strategies.[28]

[17] ISO/IEC. (Aug 2023). ISO/IEC 23837-1:2023 - Information security - Security requirements, test and evaluation methods for quantum key distribution. (see https://www.iso.org).
[18] Ministry of Science and ICT, Republic of Korea. (Jun 2023). Korea's National Quantum Strategy (see https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&bbsSeqNo=46&nttSeqNo=18).
[19] BSI. (Jan 2024). Certification Report BSI-CC-PP-0120-2024 for Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules. (see https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0120.html).
[20] European Commission. (Oct 2024). The European Quantum Communication Infrastructure (EuroQCI) Initiative (see https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci).
[21] QAssure. (2023). (see https://qassure.org/).
[22] ETSI ISG QKD was founded in 2008 with members focused on standardisation to support the creation of products and services that include QKD or consume QKD keys. A notable publication is ETSI GS QKD 014 specifying the interface between QKD and user devices (see https://www.etsi.org/technologies/quantum-key-distribution).
[23] ITU-T is also active in QKD standardisation, with a focus on recommendations for QKD networks and security under ITU-T Study Group 13 (future networks) and ITU-T Study Group 17 (security) (see https://www.itu.int/en/ITU-T/studygroups).
[24] In QKD, a trusted node is physically secure node that acts as a trusted intermediary to extend QKD network connections beyond direct links by performing key management and relay functions. ETSI. (2019). GS QKD 014 V1.1.1 Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. (see http://www.etsi.org/standards-search).
[25] Liu, Y., Zhang, W., & Jiang, C. et al. (2023). Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance Phys. Rev. Lett. 130, 210801 – Published 25 May, 2023. (see https://doi.org/10.1103/PhysRevLett.130.210801).
[26] Li, W., Zhang, L., & Tan, H. et al. (2023). High-rate quantum key distribution exceeding 110 Mb s−1. Nat. Photon. 17, 416–421. (see https://doi.org/10.1038/s41566-023-01166-4).
[27] Toshiba announces integrated PQC & QKD solution for quantum-safe networking (https://www.toshiba.eu/quantum/news/toshiba-announces-integrated-pqc-qkd-solution-for-quantum-safe-networking/)
[28] GSMA. (Oct 2024). IG 18. Opportunities and Challenges for Hybrid (QKD and PQC) Scenarios.

Annex B: Setting up the Proof-of-Concept Sandbox

Trusted Nodes

Trusted nodes have secure boundary protection against unauthorised physical intrusion into areas containing QKD/KMS equipment and links. For this PoC, the trusted nodes are located within power substations managed by SPTel that have the following three layers of physical security controls aligned with the ITU-T X.1713 recommended security requirements for the protection of QKD Nodes:

1. Server Rack Security:
   a. The server rack that houses the equipment in the trusted nodes/sites are secured with biometric authentication facilities that restricts access to only authorised personnel.
   b. In-rack devices are tagged with Radio Frequency Identification (RFID) to prevent equipment removal.
2. Room Security:
   a. Continuous video surveillance provides visual monitoring of the server racks housing the trusted nodes.
   b. Access to the room is further secured with biometric authentication, ensuring only authorised personnel can enter.
3. Site Security:
   a. The sites containing these rooms are critical information infrastructure ("CII") locations where access grants for personnel require prior security clearance and security escorts.
   b. These CII locations are protected by armed guards from security services providers and/or video surveillance and intrusion detection systems are in place to ensure site security.

The rack and room security are managed by a command-and-control facilities management system that sends proactive alarm notifications for any security breaches to the Integrated Operation Centre that monitors the nodes 24/7.

Secure Application Entity

Key consumption based on ETSI GS QKD 014 reference specification

The SAE's consumption of keys is via a standardised API interface defined by ETSI. The ETSI GS QKD 014 document specifies the communication protocol and data format for a QKD network to supply cryptographic keys to applications. This interface is implemented as a REST API, allowing application developers to make method calls to a QKD network and receive key material. For encoding posted parameters and responses, including key material, the API utilises the JavaScript object notation (JSON) data format.

Figure B-1 illustrates the key delivery flow documented in ETSI GS QKD 014 reference specification, where the SAE is the client appliance/application that requests keys and the key management entity that manages the supply of such keys.

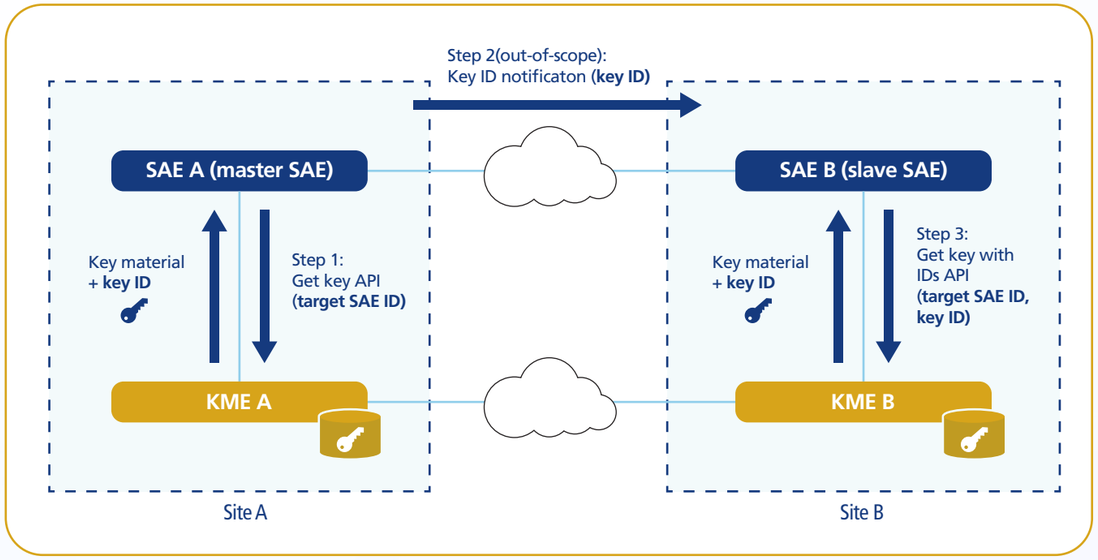

Figure B: Illustration of the key delivery flow (Source: ETSI GS QKD 014)

SAE Examples

Examples of SAEs and supporting encryption at various OSI networking layers include:

1. Dense Wavelength-Division Multiplexing (DWDM) – A Layer 1 encryption appliance used for interconnecting geographically redundant data centres, supporting encrypted network traffic at the highest bandwidth.
2. Network switch – A Layer 2 appliance utilising MACsec or custom ethernet encryptors, allowing FIs to securely bridge their local area networks (LANs) across multiple sites in a metro ethernet environment.
3. Firewall or software defined wide-area network (SD-WAN) – A Layer 3 appliance that relies on underlying IPSec tunnels to securely connect between FIs' main offices and branches.

Other SAEs may include machines or appliances incorporating hardware security modules (HSMs) that act as mediating devices to support software applications like databases, key vaults or commercial cloud infrastructure using other standardised key retrieval interfaces like Key Management Interoperability Protocol (KMIP) or Public-Key Cryptography Standards (PKCS [#11]).

HSMs, typically tamper-resistant and certified by independent labs, can create and replicate their own cryptographic keys across HSM clusters. The replication of cryptographic keys is protected by pre-shared (via out-of-band means) symmetrical keys, or PQC, or both, natively between geographically separated HSMs. This allows end customers or FIs to have full control of the cryptographic keys used in their applications or SAEs, independent of the QKD service provider. QKD keys used with network-based SAEs provide additional, quantum-safe protection for replication traffic in-transit between HSMs. This creates a defence-in-depth architecture, enhancing overall security.

Annex C: Summary of Identified Test Case Objectives and Observations

S/N	Test Case	Objectives	Observation
	Operation-focused Tests		
a	• Monitoring of QKD operational metrics, e.g. stored key count, keys per requests, key size, QKD and KMS uptime, etc	• Understand the options and metrics of concern when using the QKD as an encryption key source • Observe concepts and processes of key establishment, key storage, key consumption and refilling via metrics observed on Client Dashboard UI • Observe uptime of the QKD system and key availability over time	• The QKD dashboard displayed device health, key performance metrics and essential monitoring data, including Secure Key Rate (SKR) and Quantum Bit Error Rate (QBER)
b	• Retrieve QKD keys and keys ID		• The key retrieval process can be observed through the standardised ETSI GS QKD 014 interface (using curl command)
c	• File encryption and decryption - for single file encryption/ decryption and bulk file (i.e folder) encryption/ decryption	• Demonstrate and observe the use of global key to encrypt/decrypt the transaction file/folder, and the ability to show ciphertext (encrypt) and plaintext (decrypt) • Demonstrate that users can see which keys are being used • Demonstrate that users can observe key consumption and refill rate	• Demonstrated QKD key use for encrypting/decrypting single files and bulk folder • Displayed ciphertext, plaintext and keys used during the process • Observed key consumption and refill rates
	Security-focused Tests		
a	• Key Retrieval Errors	• Observe system response to attempted key retrieval with incorrect IP address • Observe system response to attempted key retrieval with incorrect certificate	• System failed to provide key and key ID as expected for incorrect IP and incorrect certificate • Demonstrated effective enforcement of network policies
b	• Decryption Errors	• Observe system response to attempted key retrieval with incorrect SAE ID and key ID	• Failed to retrieve keys when SAE ID and key ID is modified to a wrong value
	Operational Redundancy-focused Tests		
a	• Fibre Disconnection and Recovery of Operations • Impact Assessment of Fibre Outage on Folder Encryption	• Observe key metrics when the quantum channel is down • Observe key pool size reduction and confirm QKD key delivery occurs only via the quantum channel	• Key pool size in DMS buffer decreased when quantum channel was down • However, even with the quantum channel down such that no keys were exchanged for the duration of the test, encryption and decryption could continue using keys stored in the KMS buffer

S/N	Test Case	Objectives	Observation
	Additional Test Cases		
a	• Attempted Decryption of a QKD-encrypted File by Unauthorised Users	• Ensure that the QKD system prevents unauthorised recipients from decrypting messages	• The attempt to decrypt the QKD-encrypted file intended for a specific recipient by another unauthorised recipient was unsuccessful
b	• Perform Key Exhaustion on KMS Buffer	• Generate new keys on demand or handle requests when no keys are immediately available	• The KMS could not draw any keys for the encryptor before the designated time for the refill of the KMS buffer. It was successfully tested that after the designated time, KMS was able to draw the keys again
c	• Decryption a Double-encrypted File	• To validate the successful decryption of a file that has been encrypted twice	• Original data was successfully recovered after double decryption
d	• Use of QKD with One-Time Pad (OTP) for File Transfer	• Demonstrate the advantages of combining QKD's continuous supply of fresh key material and OTP's theoretical unbreakability, to achieve information-theoretic security in key agreement-encryption-decryption • Determine the maximum QKD key size for OTP encryption and test the practical application of QKD+OTP for encrypting and decrypting files • Assess the feasibility of using multiple concatenated QKD keys to encrypt larger files and evaluate the system's capability to handle significant data sizes	• The maximum QKD key size for OTP is 128 KB; attempts to encrypt larger files with a single key triggered errors • Files up to 128 KB were successfully encrypted and decrypted with a single QKD key each • Retrieval and concatenation of multiple keys allowed successful encryption of files larger than 128 KB • Stress tests with files of up to 500 MB in size confirmed the system's capacity for large data
e	• Use of QKD with PQC Digital Signing (ML-DSA) for File Transfer	• Evaluate the integration of QKD with PQC signing for a quantum-safe method ensuring confidentiality and authenticity	• Files successfully encrypted with AES and signed with ML-DSA • Recipients successfully verified signatures and decrypted files, confirming method effectiveness
f	• Use of QKD with PQC (ML-KEM, Classic McEliece) to establish a Quantum-Safe Virtual Private Network (VPN) Tunnel	• Evaluate the integration of QKD and PQC to establish a quantum-safe VPN tunnel, using open-source projects like Rosenpass	• Standard QKD exchange of symmetric keys successfully performed • Post-quantum key exchange successfully performed using Rosenpass, generating a matching PQC-derived key • Hybridisation of QKD and PQC keys successfully performed using HKDF algorithm • Secure VPN tunnel successfully established using pre-shared keys fed into Wireguard
g	• Use of QKD with AES-256 for an Automated SFTP File Transfer	• To test real world scenario where QKD solution can be incorporated to enhance file exchange security with minimal or no manual intervention	• Demonstrated how QKD key retrieval, data encryption / decryption, file exchange and data validation (checksum) can be incorporated in real case scenario

Annex D: Execution of Operation-focused Test Cases

Figure D-1 illustrates the process of conducting an identified core test case in the PoC, based on the operational-focused tests.

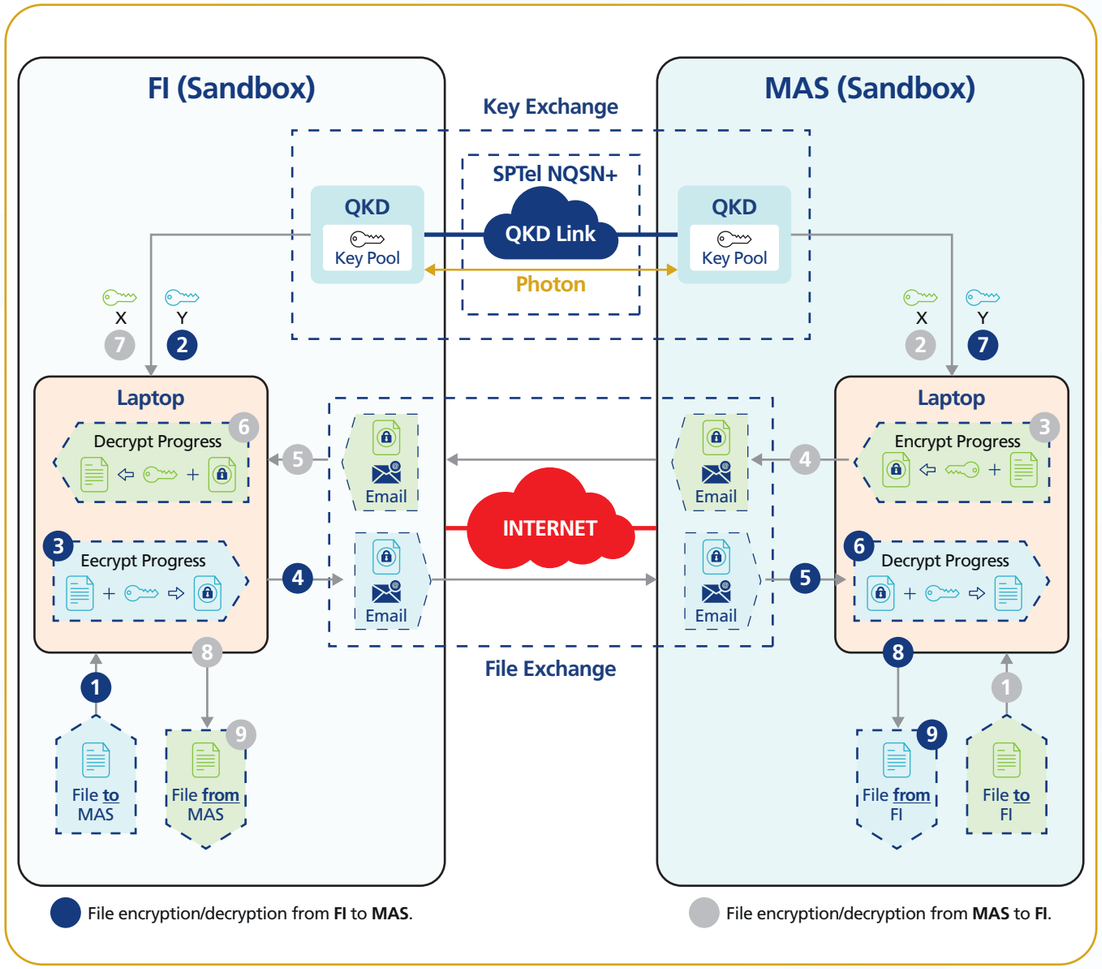

Figure D-1: Secure exchange of files between MAS and FIs via QKD SAE custom file encryption tool

Encryption Process:

Step 1: Select the File

›› Users at MAS or FI select the file(s) for encryption. Without loss of generality, let us assume that FI encrypt the file at the FI and decrypt the file at MAS. The approach outlined below works vice versa as well.

Step 2: Obtain the Encryption Key

›› The application queries for the encryption key (key and key ID) from the KMS connected to its QKD stack (issuing an ETSI GS QKD 014 call). The application also indicates that it wants to establish a key-exchange with the QKD stack at MAS. Using QKD and secure key relay through the KMS servers, key pairs are continuously generated at both the FI and MAS.

Step 3: Encrypt the File

›› Using the AES-256 algorithm, the application encrypts the file(s) using the retrieved encryption key from the KMS. Alongside the encrypted data, the key ID that is read along with the encryption key, is appended in JSON format. This key ID is an essential piece of information needed to identify the corresponding decryption key but interception of the key ID does not compromise security, as it requires proper authentication with the KMS to be useful to extract the actual decryption key.

Step 4: Share the Encrypted File

›› The encrypted file is now ready to be securely transmitted to MAS. The encrypted file is then sent over email. Even in the case of potential unauthorised access during transit, the contents remain secure and unreadable without the corresponding decryption key.

Decryption Process:

Step 5: Select the File

›› Upon receipt, user at MAS selects the encrypted file(s) they wish to decrypt.

Step 6: Obtain the Decryption Key ID

›› The application reads the key ID from the encrypted file.

Step 7: Obtain the Decryption Key

›› The application queries the KMS in its QKD stack (QKD Stack at MAS) with the key ID obtained for the same key for decryption using the same ETSI GS QKD 014 protocol, authenticated by the user's certificate.

Step 8: Decrypt the File

›› The application decrypts the file(s) using the AES-256 algorithm with the appropriately loaded decryption key, restoring it to its original form.

Step 9: Store the Decrypted File

›› The decrypted file(s) is securely stored and accessible only to authorised personnel at MAS, completing the secure transfer process.

Annex E: Additional Test Cases

Operation and Security-focused Additional Test Cases. This section provides the rationale and observation for operation and security-focused additional test cases.

i. Key Exhaustion on KMS
   - **Rationale:** Testing the system's response to key exhaustion is essential to ensure that the KMS can handle scenarios where all available quantum keys have been used. This test evaluates the robustness and scalability of the key management policies and system's ability to generate or retrieve additional keys as needed.
   - **Objective:** This includes testing the system's ability to generate new keys on demand or handle requests when no keys are immediately available. Upon key exhaustion, the system should either efficiently generate new quantum keys or queue key requests until more keys become available. The expected result is that the KMS maintains security and functionality without service interruption, demonstrating resilience and adaptability in high-demand scenarios.
   - **Observation:** After keys were aggressively exhausted (intentionally) from the KMS buffer without refilling, the KMS could not draw any keys for the encryptor before 12:00 AM (the designated time the KMS was configured to refill the buffer) on the same day. It was successfully tested that when keys were refilled the next day, keys could be drawn again.

ii. Attempted Decryption of QKD-encrypted File by Unauthorised Users
   - **Rationale:** To ensure that the QKD system strictly enforces the confidentiality of encrypted communications between specific parties, preventing unauthorised recipients from decrypting messages not intended for them.
   - **Objective:** This test aims to validate that the files encrypted for one recipient, such as a specific FI, cannot be decrypted by another. It assesses the system's capability to securely isolate the cryptographic keys and ensure that they are only usable by their intended recipient. The expected result is that one cannot use the FI's QKD system to decrypt files intended for other parties. This test verified the effectiveness of the system's security measures to prevent cross-decryption of files, ensuring that each recipient can only access data meant for them.
   - **Observation:** The attempt to decrypt the QKD-encrypted file intended for a specific recipient by another recipient was unsuccessful. The system effectively enforced the confidentiality of the encrypted communications, preventing unauthorised access. This confirms that the QKD system successfully isolates cryptographic keys, ensuring that only the intended recipient can decrypt the files. The test was passed as anticipated, validating the effectiveness of the system's security measures against cross-decryption.

iii. Decrypt a Double-encrypted File
   - **Rationale:** In scenarios where sensitive information is stored, double encryption can provide an additional layer of security. Testing the decryption process ensures that the data can be retrieved accurately while maintaining its confidentiality. It is essential to confirm that the entire encryption and decryption workflow operates as intended. This includes verifying that the system can handle files that have undergone multiple encryption processes, which is critical for applications that require high security.
   - **Objective:** To validate the successful decryption of a file that has been encrypted twice, ensuring that both encryption layers can be effectively reversed to retrieve the original data without loss or corruption.
   - **Observation:** Original data was successfully recovered after double decryption. MD5 and SHA checks were conducted and the checksums were consistent with the original file.

Advanced Cryptographic Applicability Additional Test Cases. This section provides the rationale, observation and processes for conducting advanced cryptographic applicability additional test cases.
A total of four advanced cryptographic applicability tests were identified, with the rationale and observations as follows:

i. Use of QKD with One-Time Pad (OTP) Encryption for File Transfer

   The use of QKD with OTP encryption was evaluated to explore its potential as a cryptographic solution which provides information-theoretic security. OTP is renowned for providing theoretically unbreakable encryption using keys that are at least as long as the message itself and never reused. Unlike traditional encryption methods such as AES which do not achieve the perfect secrecy of OTP, the combination of QKD and OTP offers a critical advantage in this respect. QKD can deliver a continuous supply of fresh key material as required by OTP and being theoretically unbreakable itself, the combination of QKD and OTP (OTP+QKD) forms a comprehensive key distribution-encryption-decryption framework resistant to current and future threats. Consequently, QKD+OTP is an attractive solution for transmitting highly sensitive information, although it may not be suitable for high-bandwidth connections due to QKD's bit rate limitations which depend on the device's capacity and the distance from trusted nodes. With the increasing need for robust cryptographic strategies, there is an opportunity to extend the adoption of OTP by leveraging the deployment of QKD networks.

   The test began by determining an appropriate QKD key size for One-Time Pad (OTP) encryption, which requires the key to match the length of the message. Initial tests focused on encrypting and decrypting files up to 128 KB using OTP with QKD-derived keys. These files were successfully processed through XOR operations, demonstrating the viability of QKD for secure encryption in OTP use cases.

For larger files, a method was implemented to retrieve and concatenate multiple QKD keys to match the required message length. Key identifiers were embedded in the metadata to ensure the recipient could reconstruct the key sequence accurately for decryption. This technique was validated through successful encryption and decryption of larger files. Stress testing extended up to 500 MB, confirming the system's ability to support high-volume data encryption using continuous key retrieval and coordinated key management.

These tests collectively demonstrated the viability and robustness of using QKD for OTP encryption for a wide range of encryption needs, from small to large-scale data transmission, highlighting both the potential and operational considerations of such a robust cryptographic solution. We note that with QKD we may even be able to use OTP to encrypt a voice call at a rate of 64 kbps. Moving forward, using OTP encryption with QKD in well-known protocols would still require some work to adapt said protocols.

Encryption Process:

Step 1: Select a File for Encryption

- User selects the file they wish to encrypt.

Step 2: Read and Pad File Data

- The application reads the selected file in binary mode to determine its original size. It then adds padding to the data to ensure the total length is a multiple of 8 bytes. This is necessary because encryption algorithms often require data blocks to be of a specific size and padding ensures that the data aligns with these block boundaries.

Step 3: Calculate Key Size Requirements and Determine Number of Key Pulls

- The application calculates the total key size needed based on the padded file size. Given that each key retrieved can be a maximum of 128 KB (1048576 bits), the script divides the total key size by 128 KB and pads accordingly to a length that is of multiples of 8. This ensures there is sufficient key material to cover the entire file, as OTP encryption requires the key to be at least as long as the data being encrypted.

Step 4: Retrieve Encryption Keys

- For each required key pull, the application makes an ETSI GS QKD 014 API call using a curl command to retrieve the key and key ID from the KMS, specifying each key size to be 128 KB. After pulling enough number of keys, the keys obtained are decoded from base64 and concatenated to form a complete encryption key.

Step 5: Encrypt the Data and Tag the Key ID

- The application performs XOR operations on the padded file data using the concatenated encryption key. Following encryption, the key IDs used are encoded and appended to the encrypted data as a tag, which is essential for identifying the correct keys during the decryption process.

Step 6: Save Encrypted File

- The resulting encrypted data, along with the appended key ID tag, is saved to a new file with a ".encrypted" extension. The encrypted file is now ready to be securely transmitted to the recipient.

Decryption Process:

Step 7: Select a File for Decryption

- The recipient selects the file they wish to decrypt.

Step 8: Read Encrypted Data and Extract Tag

- The application reads the encrypted file in binary mode to access the encrypted data. It identifies and extracts the appended tag, which contains the key IDs. These key IDs are crucial for retrieving the correct decryption keys from the KMS.

Step 9: Retrieve Decryption Keys

- For each key ID extracted from the tag, the application performs a similar ETSI GS QKD 014 API call to retrieve the corresponding key. The retrieved keys are decoded from base64 and concatenated to form a complete decryption key.

Step 10: Decrypt the Data

- The application decrypts the file(s) using the AES-256 algorithm with the appropriately loaded decryption key, restoring it to its original form.

Step 11: Remove Padding

- After decryption, the application removes any padding that was added during the encryption process. This step ensures that the decrypted data matches the original file size and content, eliminating any additional bytes that were introduced for alignment purposes.

Step 12: Save Decrypted File

- The resulting decrypted data is saved to a new file with a ".decrypted" extension, replacing the ".encrypted" suffix. This step completes the secure transfer process.

ii. <u>Use of QKD with Post-Quantum Cryptography (PQC) Digital Signing for File Transfer</u>

The test aimed to address the limitations of QKD, which, while capable of providing confidentiality and integrity through a Message Authentication Code (MAC), lacks the initial trust establishment that asymmetric cryptography via certificates, offers. PQC algorithms are designed to remain secure against both classical and quantum attacks by relying on complex mathematical problems. These algorithms run entirely on classical hardware and aim to replace vulnerable public-key cryptosystems like RSA and ECC, which are susceptible to quantum algorithms such as Shor's. By employing the PQC digital signature algorithm ML-DSA and available from open-source libraries, this approach demonstrated the importance of using quantum-safe digital signatures to protect files against tampering and forgery.

The process involved encrypting a file with AES using a QKD key and then signing it with the ML-DSA algorithm, resulting in a set of encrypted file, a signature file and a public key. The sender transmitted these files to the recipient, who verified the signature with the public key to confirm authenticity and integrity, then decrypted the file using the QKD key. The successful execution of these steps by both parties demonstrated the effectiveness of combining QKD with PQC signing to ensure both data confidentiality and authenticity. While we did not use any PQC certificate, this was a step toward using QKD for enhanced security with authenticity using PQC digital signatures.

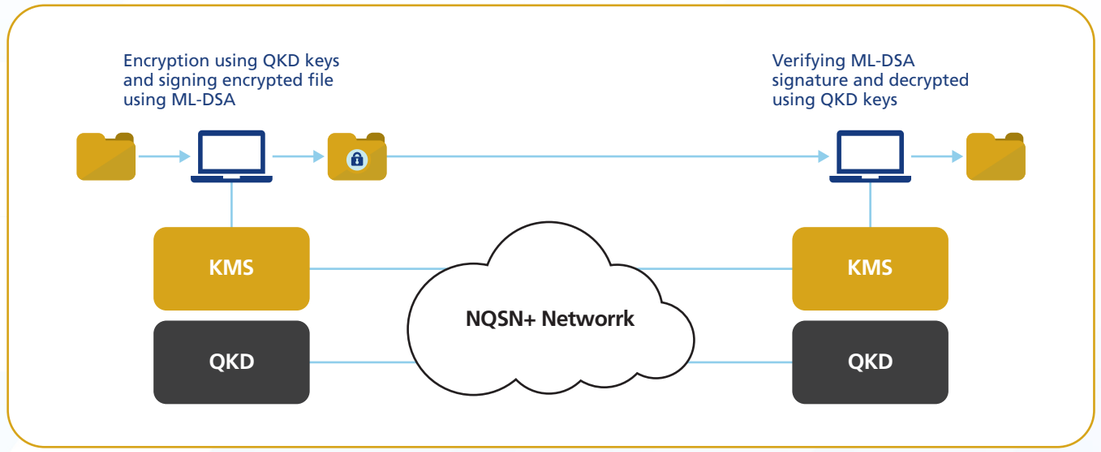

Figure E-1: Setup for using QKD for file encryption and PQC digital signing

Encryption Process:

Step 1: Select a File for Encryption

›› User selects the file they wish to encrypt.

Step 2: Retrieve Encryption Key

›› The application queries for the encryption key (key and key ID) from the KMS connected to its QKD stack (issuing an ETSI 014 call).

Step 3: Encrypt the Data and Tag the Key ID

›› The application reads the selected file in binary mode and uses the retrieved key with the AES encryption scheme to encrypt the data. The key is then zeroised in memory for security. Following encryption, the key IDs used are encoded and appended to the encrypted data as a tag, which will be essential for identifying the correct keys during the decryption process.

Step 4: Save Encrypted File

›› The tagged encrypted data is saved to a new file with a ".encrypted" extension.

Step 5: Sign the Encrypted File

›› The application generates a digital signature for the encrypted file using the PQC ML-DSA algorithm. The signing process involves creating a signature with the private key, while the corresponding public key is saved to a file. This public key belongs to the sender and is necessary for the recipient to verify the integrity and authenticity of the encrypted file. Once the encryption and signing are complete, the encrypted file, the signature file and the public key file must all be sent to the recipient. This ensures that the recipient has all the necessary components to verify the file's authenticity and proceed with decryption.

Decryption Process:

Step 6: Receive and Select Files for Decryption

›› Upon receiving 3 files: the encrypted file with a ".encrypted" extension, the corresponding signature file with a ".signature" extension and the sender's public key file, the recipient launches the application and selects the file they wish to decrypt.

Step 7: Verify Signature

›› The application verifies the digital signature of the encrypted file using the public key and the signature file to ensure the integrity and authenticity of the encrypted data. This step confirms that the file has not been tampered with and is indeed from the sender.

Step 8: Extract Key ID

›› The application reads the encrypted file data and identifies the appended tag. It extracts the key ID from this tag, which will be necessary for retrieving the correct decryption key.

Step 9: Retrieve Decryption Key

›› The application performs a similar ETSI GS QKD 014 API call to retrieve the corresponding key from the KMS.

Step 10: Decrypt the Data

›› With the correct decryption key retrieved, the application uses the AES encryption scheme to decrypt the data. Upon successful decryption, the key is zeroised in memory for security and the decrypted data is saved to a new file with a ".decrypted" extension.

iii. <u>Setting up a hybridised QKD-PQC to establish a Quantum-Safe Virtual Private Network (VPN) Tunnel</u>

Resilience is a cornerstone of the transition to quantum-safe security. Given the profound and transformative nature of this shift, organisations should seize the opportunity to move beyond minimal compliance by adopting strategies and technologies that ensure operational continuity despite evolving threats. One effective approach is to combine complementary technologies—so that if one fails, the other still maintains protection. For example, both PQC and QKD can be deployed at the same layer, such as Layer 3 of the OSI model, to secure a VPN tunnel. In this configuration, if a future vulnerability is discovered in a PQC algorithm or a flaw in QKD implementation emerges, the overall system remains protected.

This test aimed to validate the integration of QKD and PQC for establishing a quantum-safe VPN tunnel. It drew inspiration from Project Arnika[29], developed by Cancom Converged Services under the EU EUROQCI / QCI-CAT program, specifically for the "HSM Backup Using QKD" use case. The implementation featured a compact and lightweight external extension to WireGuard VPN, designed to incorporate symmetric keys as Pre-Shared Keys (PSKs) into the WireGuard protocol.

[29] Arnika is a compact, lightweight external extension for Wireguard VPN, engineered to incorporate symmetric keys as Pre-Shared Keys (PSK) into Wireguard. It gathers a 256-bit symmetric encryption key from a KMS within a QKD infrastructure (see https://github.com/arnika-project/arnika).

A critical component of the setup was the Rosenpass[30] engine, which utilises two PQC algorithms (Classic McEliece and ML-KEM) to establish a PQC-secured key. The process involved a standard QKD key exchange, where symmetric keys were securely generated and synchronized between parties. In parallel, Rosenpass was used to perform a PQC-based key exchange, ensuring both endpoints derived matching PQC keys. These QKD and PQC keys were then combined using the HMAC-based Key Derivation Function (HKDF) to produce a hybrid key. This derived hybrid key was configured as a PSK in WireGuard, successfully enabling the establishment of a highly secure VPN tunnel, resilient to both classical and quantum threats.

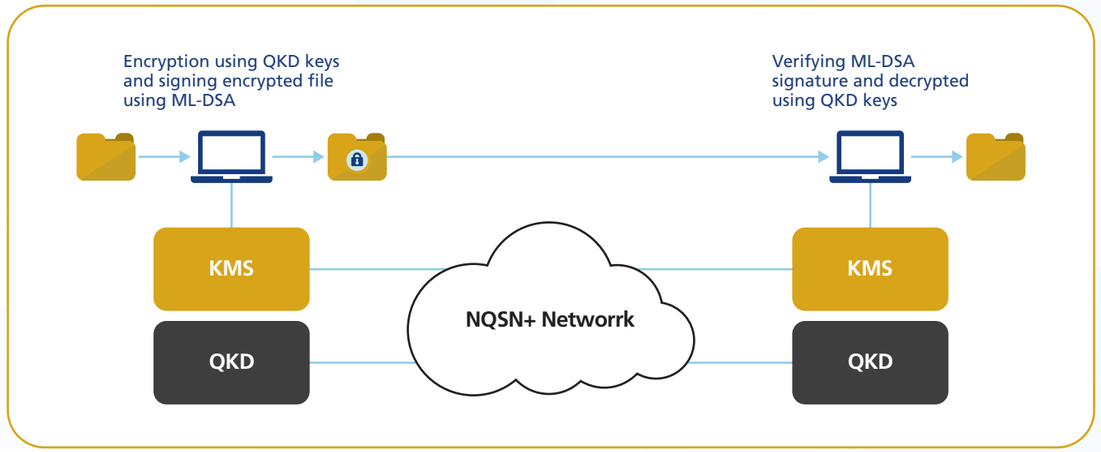

Figure E-1: Setup for using QKD for file encryption and PQC digital signing

To establish a quantum-safe VPN tunnel between FI and MAS, virtual machines running on Microsoft's Hyper-V virtualisation software were set up on both ends, using a Linux-based operating system. The necessary software installations include Rosenpass for PQC key exchange and WireGuard for managing the encrypted VPN tunnel, along with a customized program to perform key hybridization of QKD and PQC keys. Communication between FI and MAS is initiated via a WebSocket ping, where FI actively pings to start the process and MAS passively listens, ready to respond through a scripted service.

Step-by-Step Protocol

Step 1: MAS Listens for Initiation

›› MAS runs a listening script that continuously waits for a WebSocket ping from FI. This script ensures MAS is always ready to respond as soon as FI initiates the communication.

Step 2: FI Initiates Handshake

›› FI runs a script that sends a WebSocket ping to MAS to trigger the setup process. Upon receiving acknowledgment from MAS, FI proceeds with the QKD and Rosenpass operations.

Step 3: FI Retrieves QKD Key

›› oFI performs an ETSI API call to retrieve the QKD key and key ID from the KMS, then sends the key ID to MAS through an established communication channel.

Step 4: MAS Retrieves Matching QKD Key

›› oMAS queries its KMS for the QKD key that corresponds to the received key ID. Now, both FI and MAS possess the same symmetric QKD key.

Step 5: Rosenpass Post-Quantum Key Exchange

›› TFI and MAS execute the Rosenpass engine to carry out a PQC-based key exchange. This results in a shared PQC key between FI and MAS.

Step 6: Hybrid Key Derivation with HKDF

›› FI and MAS combine their QKD and PQC keys using the HMAC-based Key Derivation Function (HKDF). A hybridised key is created.

Step 7: WireGuard Pre-Shared Key Configuration and Handshake

›› The hybridised key is fed into WireGuard as the Pre-Shared Key (PSK). During the handshake, FI and MAS use each other's WireGuard public keys to verify identities.

Step 8: VPN Tunnel Established

›› Once both nodes complete the WireGuard handshake, a secure VPN tunnel is established. The derived session key, based on the PSK, ensures encrypted communication through the tunnel.

[30] Rosenpass. (see https://rosenpass.eu/docs/rosenpass-project/whitepaper/)

iv. <u>Use of QKD with AES-256 for an automated file transfer leveraging Secure File Transfer Protocol (SFTP)</u>

This test aimed to simulate real-life file transfers using today's existing applications which leverages SFTP for automated processes, unlike previous operation-focused tests that involved manual file transmission via email. A programme was developed for the sender to automatically request encryption keys from the QKD service via ETSI GS QKD 014 API, use these keys to encrypt the file with AES-256, and upload the encrypted file to the SFTP server along with a checksum for integrity verification. On the recipient's side, the programme automatically downloads the encrypted file from the SFTP server to their local environment, verifies its integrity using the SHA-256 checksum and retrieves decryption keys from the QKD service to decrypt the file. The automated key retrieval process ensures secure and efficient handling by following a "use and forget" policy, minimising the risk of key storage vulnerabilities.

Encryption Process:

Step 1: Select a File for Encryption

›› Sender runs a script to identify the list of parameters required such as the recipient, file to encrypt, etc.

Step 2: Obtain the encryption key

›› The script calls for the encryption key (Key + Key ID) from the KMS connected to its QKD stack (issuing an ETSI GS QKD 014 call).

Step 3: Encrypt the File

›› The script encrypts the file using the encryption key obtained from the KMS and Key ID is appended in the encrypted file.

Step 4: Upload to SFTP server

›› The script uploads the file to the SFTP server registered.

Step 5: Create checksum

›› The script generates an additional checksum for file integrity check.

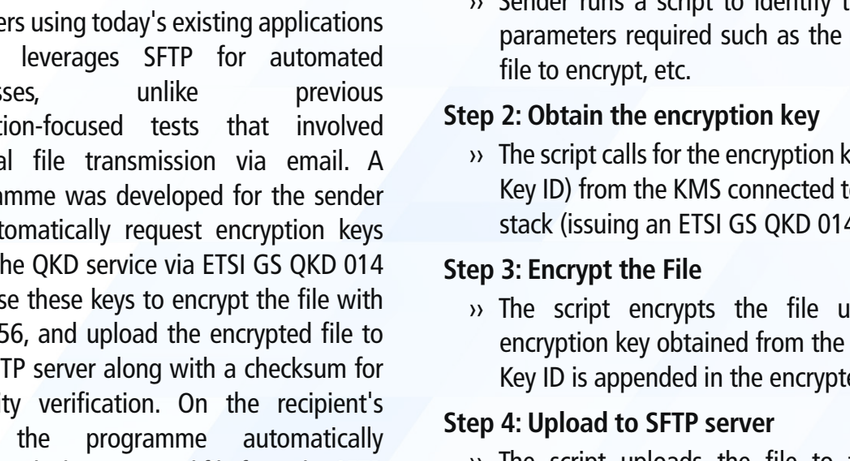

Figure E-3: Encryption process for use of QKD with AES-256 for an automated file transfer leveraging SFTP

Decryption Process:

Step 1: Select a File for Encryption

›› Recipient runs a script to identify the list of parameters required such as the sender, file to decrypt, etc.

Step 2: Download from SFTP server

›› The script downloads the encrypted file from the SFTP server registered.

Step 3: Extract Decryption Key ID

›› The script extracts the Key ID embedded in the encrypted file.

Step 4: Get Decryption Key

›› The script calls for the decryption key from the KMS connected to its QKD stack (issuing an ETSI 014 call with the Key ID obtained).

Step 5: Decrypt the file

›› The script decrypts the file using the decryption key obtained from the KMS.

Step 6: Create checksum

›› The script generates an additional checksum for file integrity check.

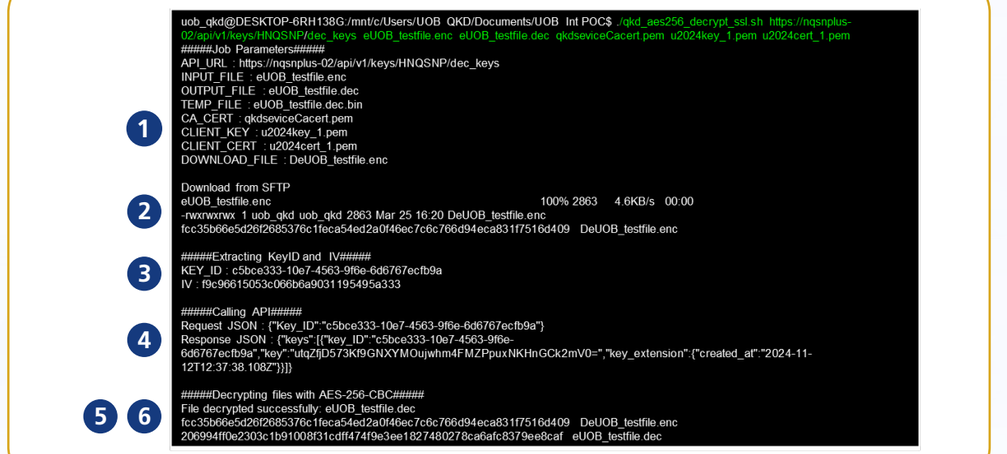

Figure E-4: Decryption process for use of QKD with AES-256 for an automated file transfer leveraging SFTP

Annex F: Project Committees

The members of the project committees can be found below.

Steering Committee

S/N	Name	Organisation
1	Tan Yeow Seng	MAS
2	Damien Pang	MAS
3	Ang Li Khim	DBS
4	Heng Kim Chwee	DBS
5	Lee Mun Liong	HSBC Singapore
6	Alejandro R.-P. Montblanch	HSBC
7	Thomas Low	OCBC
8	Robin Foe	OCBC
9	Lee Yeong Chee	UOB
10	Murari Kalyanaramani	UOB
11	Lum Chune Yang	SpeQtral
12	Cyril Tan	SpeQtral
13	Titus Yong	SPTel
14	Susan Loh	SPTel

Working Committee

S/N	Name	Organisation
1	Lim Tong Lee	MAS
2	Claudean Zheng	MAS
3	Chee Kin Ban	MAS
4	Eng Gun Kiat	MAS
5	Philip Loy	MAS
6	Aman Singhal	MAS
7	Edwin Goh	MAS
8	Elvina Woo	MAS
9	Ashwin Surendran	MAS
10	Chan Jyh Chyang	MAS

Working Committee

S/N	Name	Organisation
11	Deng Yihan	MAS
12	Naomi Sago	MAS
13	Tan Kok Loong	DBS
14	James Chan	DBS
15	Raydon Thor	DBS
16	Walter Cheung	DBS
17	Koh Sin Huat	HSBC Singapore
18	Cheryl Tanaja	HSBC Singapore
19	Phyllis Liau	HSBC Singapore
20	Yap Hong Oon	HSBC Singapore
21	Sripal Jain	OCBC
22	Ryan Zhang	OCBC
23	Patrina Wong	OCBC
24	Lionel Tan	OCBC
25	Michelle Teo	UOB
26	Omeila Fun	UOB
27	Philip Ng	UOB
28	Lim Buk Nguang	UOB
29	Hla Min	UOB
30	Cyril Tan	SpeQtral
31	Robert Bedington	SpeQtral
32	Alexander Dixon	SpeQtral
33	Edward Guyot	SpeQtral
34	Jeshua Lin	SpeQtral
35	Joanne Liao	SpeQtral
36	Heng Kwee Tong	SPTel
37	Yong Hai Hung	SPTel
38	Wang Kangni	SPTel