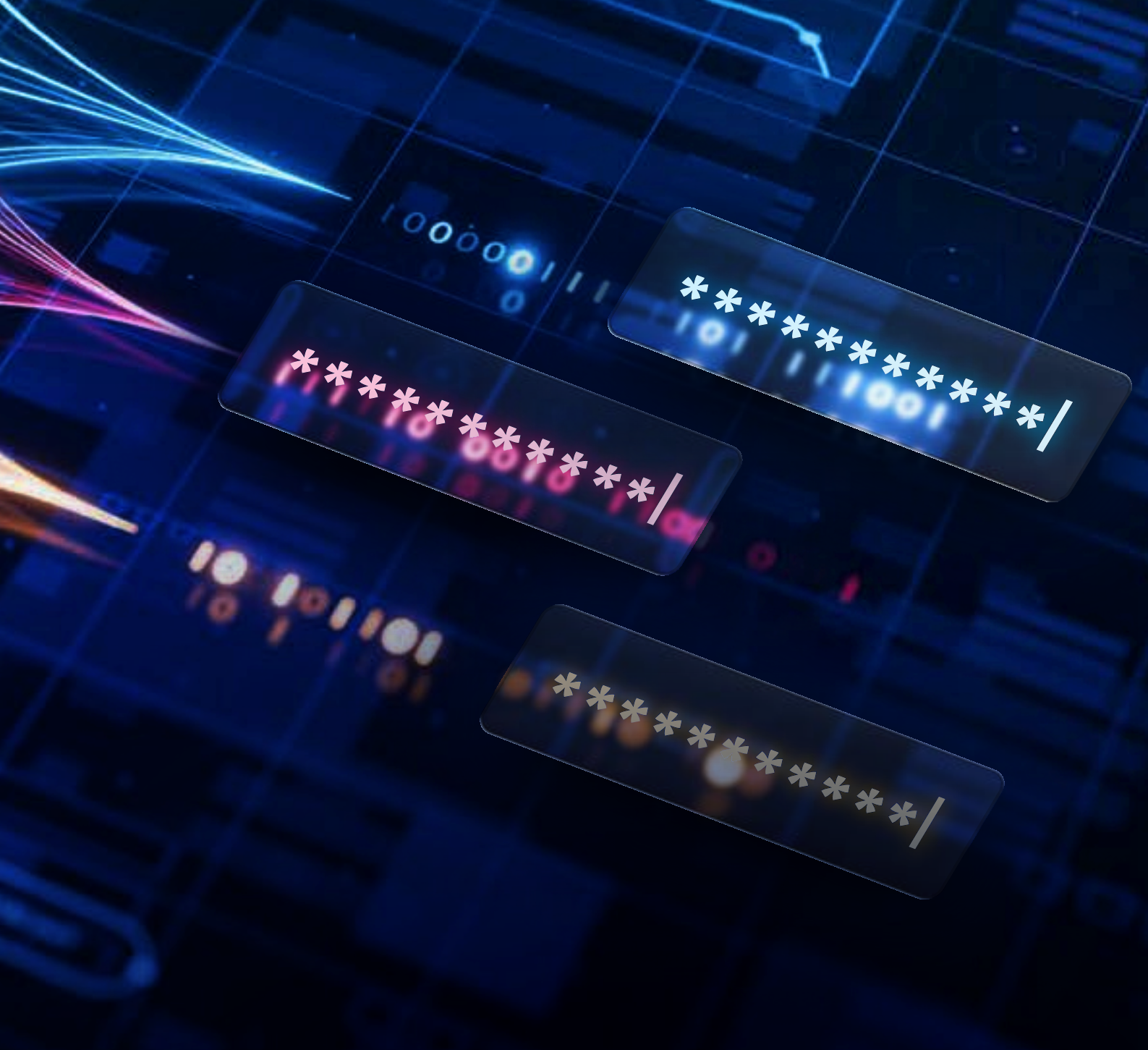


The background is a dark blue digital landscape. It features a line graph with a wavy line, a circular gauge showing '68%', and several horizontal bars of varying lengths. On the right side, there are vibrant, multi-colored light trails (blue, purple, orange) that curve upwards. In the lower-left area, there are three rectangular panels containing binary code (0s and 1s) and asterisks. The NCS logo is in the top-left corner.

nCS //



**Preparing for a
quantum-safe future:
A practical guide**



Authors

Ying Shao Wei (NCS)
Chief Scientist

Vijay Nayudu (NCS)
AI Business Lead

Hoon Wei Lim (NCS)
Principal Director,
Cyber Special Ops - R&D

Choon Hock Niow (NCS)
Lead Consultant,
Cyber Special Ops - R&D

Nay Oo (NCS)
Lead Data Scientist,
Cyber Special Ops - R&D

Contents

01	Introduction • Why quantum matters now • The urgency for enterprises • About this guide	4
02	Part 1: Preparing for a quantum-safe future • Strategic context and the case for PQC migration • Figure 1: Statistics on the pervasiveness of cryptography • A proactive migration roadmap • Figure 2: A proactive migration strategy • The business case for acting early	6
03	Part 2: Automating discovery of cryptographic assets • The hidden challenge of cryptographic sprawl • Why automation matters • Figure 1: High-level architecture of an automated discovery of cryptographic assets • From visibility to action	14
04	Part 3: Security validation of Quantum Key Distribution Networks • The challenge of validating new technologies • NCS's validation approach • Results and enterprise impact • Conclusion: Confidence through validation	21
05	The path forward • From strategy to action • Why timing matters • The role of NCS	26
06	References	27



Introduction

Why quantum matters now

Quantum computing is no longer confined to research labs and theoretical discussions. With global investment accelerating, breakthroughs are happening at a pace that outstrips expectations. While this progress brings exciting opportunities, it also creates one of the most significant cybersecurity risks in decades: the potential to break today's widely used encryption methods.

RSA, ECC, and other algorithms that protect everything from financial transactions to healthcare records could be rendered vulnerable once quantum computers reach maturity. The danger is not limited to the future; adversaries are already engaging in "harvest now, decrypt later" attacks, storing encrypted data today with the intent of unlocking it tomorrow.

The urgency for enterprises

For business leaders, this is more than a technical challenge. Failure to act could undermine customer trust, disrupt operations, and lead to compliance breaches. Just as digital transformation reshaped competitive landscapes, quantum disruption will define resilience and confidence in the years ahead.

About this guide

In the following pages we bring together three interconnected perspectives to help organisations prepare for a quantum future. Together, these three parts create a structured journey, from strategic context to practical discovery, to technical validation.

Part 1: Preparing for a quantum-safe future

A broad overview that explains why Post-Quantum Computing (PQC) matters now and the proactive migration roadmap forward.

Part 2: Automating discovery of cryptographic assets

A practitioner-focused deep dive into one of the toughest challenges of migration: identifying where cryptography actually lives within your systems.

Part 3: Security validation of Quantum Key Distribution Networks

A technical case-style study showing how NCS validates quantum-era security technologies in real-world conditions.

By reading this guide, you will:

- Understand why PQC migration is a strategic business priority, not just an IT task.
- See how automated discovery tools provide the foundation for large-scale migration.
- Learn how rigorous validation gives enterprises the confidence to adopt next-generation security technologies.

Most importantly, you will gain a clearer picture of how your organisation can start preparing today ensuring resilience, trust, and continuity in a quantum-enabled future.

Part 1: Preparing for a quantum-safe future

Executive summary

Quantum-safe cryptography standards have recently been released. Implementation of these standards will be a cornerstone for organisations to defend against quantum threats that expose today's sensitive data in the future, known as “harvest now, decrypt later”. Early preparation enables organisations to assess and upgrade their cryptographic landscape systematically, ensuring that their data and communications remain secure and resilient against attacks based on cryptographically relevant quantum computing.

In the following pages, we will present a proactive migration strategy, covering the “when” and “how” questions, that allows organisations to be better positioned to start their transition to a quantum-safe state cost-effectively, and develop the capability to manage various challenges that may arise throughout the transition.

Cryptography is everywhere

In today's digital age, cryptography is deeply woven into our daily lives yet often goes unnoticed by users. Take WhatsApp's 2.9 billion active users [Cec24] for example—end-to-end encryption secures their messages without them needing to think about it. Beyond messaging, web interactions like browsing or online banking rely on cryptographic protocols to protect data. More than 94% of today's web traffic is encrypted, safeguarding data exchanged over the Internet [Goo24].

Identity management also heavily relies on cryptography. For instance, single sign-on (SSO) systems use digital signatures to verify user identities and encrypt passwords to prevent unauthorised access. Our smartphones are another example; applications like Singpass secure personal information and authentication data, while biometric data (such as fingerprints or facial recognition) is protected through encryption to prevent leaks or misuse. Figure 1 provides some statistics on the use of cryptography in various applications.

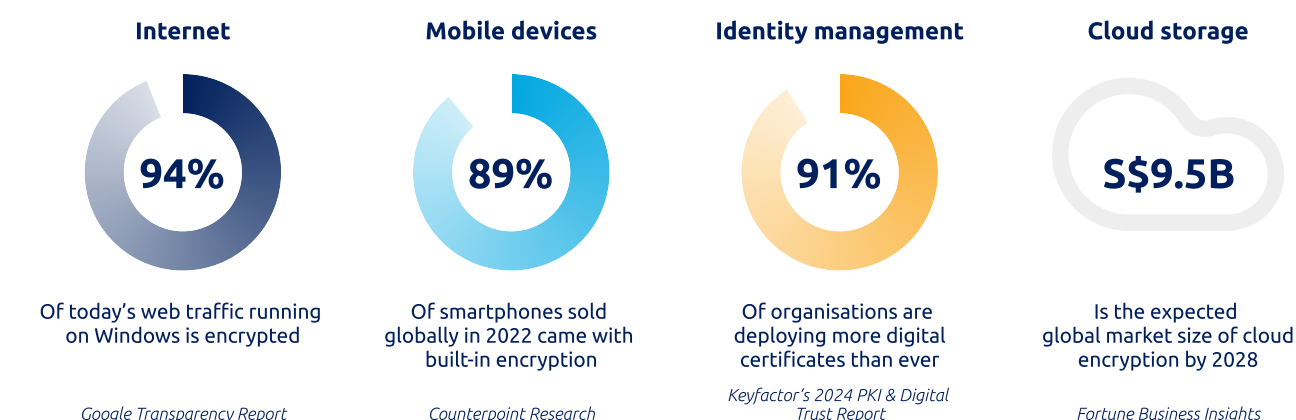


Figure 1: Statistics on the pervasiveness of cryptography.

The use of cryptography is widespread for two reasons:

1. Data confidentiality and integrity

Cryptography plays a vital role in ensuring that data is not only kept private but also remains unchanged during transmission. For example, digital signatures provide authenticity and integrity, ensuring that the data comes from a trusted source and hasn't been tampered with.

2. Multi-layer defence strategy

In a robust cybersecurity framework, multiple layers of defence are employed across infrastructure, networks, systems, and data. At the data layer, cryptography acts as the last line of defence. Even if other security controls fail, encryption keeps sensitive data protected from unauthorised access or exposure.

As digital technology becomes more integral to our daily lives, cryptography's role in protecting sensitive information, verifying identity, and ensuring secure communication continues to expand. It remains the invisible guardian of our data, offering a critical layer of security in our interconnected world.

Why is Post-Quantum Cryptography (PQC) a big deal?

Cryptography is the foundation of cybersecurity, protecting everything from personal messages to financial transactions. Despite its omnipresence, many of us underestimate its critical role. In a multi-layered defence strategy, cryptography acts as the last line of defence, safeguarding data even if other security layers, such as networks or systems, are compromised.

However, there's a growing challenge: most cryptographic algorithms can be broken, given enough time and computing power. This is why Post-Quantum Cryptography (PQC) is such a big deal, and not just because of the looming threat of quantum computing.

The growing vulnerability of cryptography

Most modern cryptographic methods are built on mathematical principles that were once considered unbreakable. Take SHA-1, for example. It was once the standard for securing passwords and sensitive data, transforming them into random strings to keep them secret. However, with advancements in computing power, such as powerful GPUs, an 8-character password protected by SHA-1 can now be cracked within one hour using brute-force attacks [Nes24].

This is a clear example of how cryptographic algorithms become vulnerable over time as technology advances. It's not just about quantum computers; even today's systems, like next-generation GPUs with AI capabilities, could potentially break many widely used encryption techniques.



Why PQC matters beyond quantum threats

While quantum computing is often viewed as the primary threat to existing cryptography, PQC addresses broader security concerns. Modern cryptography inherits specific mathematical properties that introduce potential vulnerabilities. It's only a matter of time before someone devises a new algorithm or technique to break today's cryptographic systems much faster than brute-force methods.

For example, if companies like Nvidia develop the next generation of AI-powered GPUs that can perform attacks far faster than current hardware, cryptographic methods that are secure today might become obsolete tomorrow.

Recognising these risks, the National Institute of Standards and Technology (NIST) has spent the past 8 years working on PQC. In collaboration with academic and industry researchers, they carefully reviewed and improved new PQC algorithms based on a diverse range of mathematical theories. Their goal was to address the weaknesses and limitations of today's cryptographic systems, drawing on lessons from the past four decades.

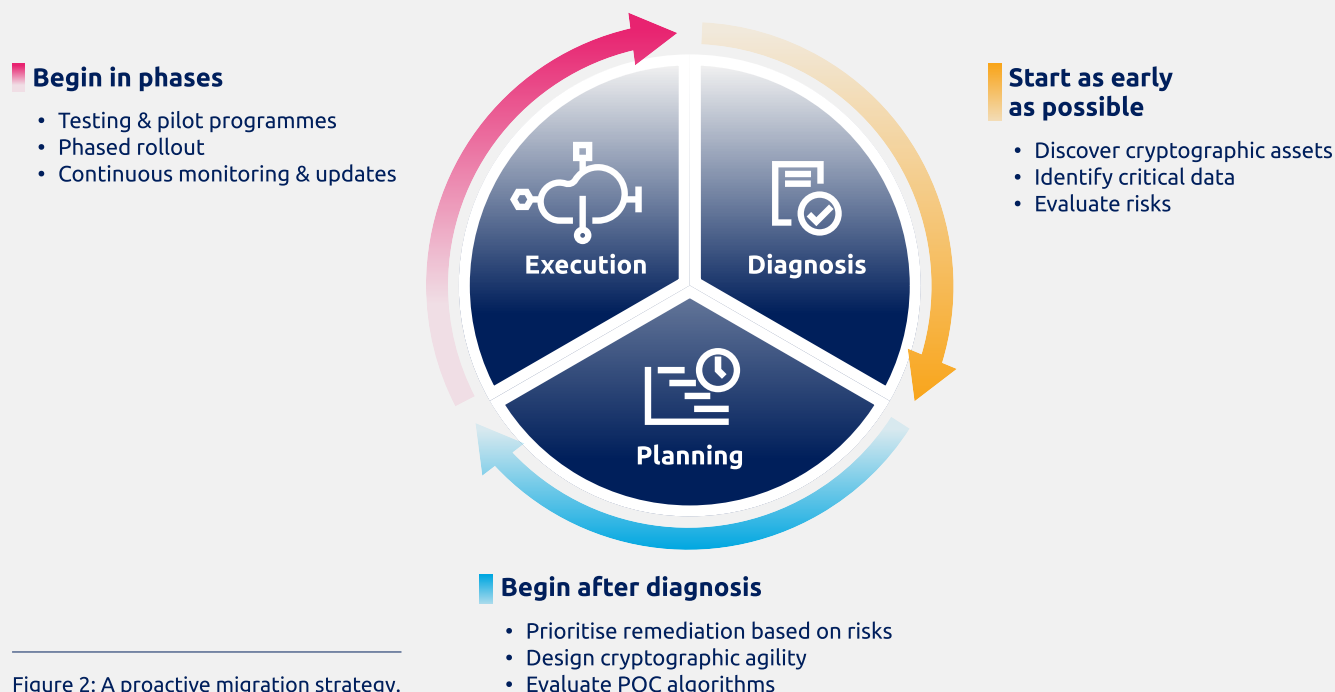
Adopting PQC is about embracing stronger, more secure, and more flexible cryptography by diversifying our reliance on different algorithms, ensuring a more robust defence against future threats. This is akin to putting our eggs into multiple baskets, diversifying the algorithms we rely on to avoid over-dependence on a single cryptographic method.

While quantum computing represents a significant threat to cryptographic systems, it's just one example of how advancements in computing power can compromise today's security. The reality is that new technologies, like high-performance processors or AI-driven systems, could develop methods that break cryptographic algorithms far more efficiently than brute-force attacks.

Just as we saw with SHA-1, cryptographic systems that seem secure today may quickly become vulnerable. That's why adopting PQC isn't just about preparing for quantum computers—it's about preparing for any future threat that could undermine our current cryptographic methods.

A proactive migration strategy

Successfully migrating to quantum-safe cryptography requires a well-thought-out strategy that addresses both the technical and operational challenges. The following roadmap outlines a practical and cost-effective approach to the migration process, as illustrated in Figure 2.



Diagnosis

The diagnosis phase is foundational and should be started as early as possible. It involves identifying all aspects of the organisation's cryptographic use. This includes understanding where and how data is protected—whether in databases, during network transfers, or within secure applications. The goal is to create a comprehensive overview of where cryptography is applied and to understand which systems require early migration to PQC. Here is a breakdown of key activities in this phase:

Inventorise cryptographic assets

List all applications, services, and protocols that currently use cryptography. Identify the type of cryptographic algorithms in use (e.g., RSA, ECC) and the associated key lengths.

Identify high-value data

Identify critical business processes and determine which data assets are most sensitive, such as customer records, financial information, or intellectual property. Consider how long this data needs to remain secure.

Evaluate risks

Since the “harvest now, decrypt later” strategy is a primary concern, consider the lifespan of data and the time frame within which it must remain protected. Data that requires long-term confidentiality is more vulnerable to quantum decryption.

A comprehensive diagnosis must take into account the following key considerations:

Legacy systems and unidentified cryptography

Many organisations utilise legacy systems that employ cryptographic protocols without comprehensive documentation. Discovering these cryptographic usages requires thorough analysis, including code inspection and network traffic analysis using different types of tools.

Supply chain and third-party dependencies

A comprehensive diagnosis requires considering not only internal systems but also dependencies on third-party services and vendors, which may also utilise vulnerable cryptographic protocols.

By performing these diagnostic steps, organisations can clearly understand their current cryptographic state, its vulnerabilities, and the implications of quantum threats.

Planning

The planning phase is all about developing a well-structured roadmap for the migration to PQC. This phase should begin once the diagnosis phase is complete and enough information has been gathered about where cryptography is applied. The planning phase should:

Prioritise remediation based on risks

Using the data collected during diagnosis, categorise systems based on their sensitivity, criticality, and exposure to quantum threats. Systems protecting long-lifetime data should be prioritised.

Design cryptographic agility

Cryptographically agile designed systems can easily switch between classical and quantum-safe algorithms. This will allow for smooth transitions as standards evolve and the threat landscape changes.

Educate stakeholders

Planning a PQC migration isn't just a technical endeavour—it involves many stakeholders, including IT, security, compliance, and leadership. These stakeholders need to understand the implications of PQC and support the migration strategy.

Evaluate the suitability of PQC algorithms

Since multiple PQC algorithms exist for encryption, signatures, and key exchange, choose algorithms that suit your performance, security, and compatibility requirements. Testing these algorithms in real-world scenarios can reveal integration and performance issues.

Two key factors to consider in planning are:

1. Compliance and standards

Ensure alignment with emerging PQC standards and any regulatory requirements. For example, organisations should follow guidelines published by NIST or relevant governmental bodies to ensure their cryptographic practices are compliant.

2. Performance impact and compatibility

Consider how PQC algorithms may impact system performance, as many PQC solutions have larger key sizes and computational requirements. Testing and validating performance impacts are essential to ensure that critical operations are not hindered.

By carefully planning the transition, organisations can ensure that the PQC migration is phased, prioritised based on risk, and aligned with broader business goals and regulatory requirements.

Execution

This is the most critical phase, where plans are put into action. It is essential to begin execution in phases to ensure that systems remain secure while minimising operational impact. Here are key strategies for the execution phase:

Pilot programs and testing

Start by implementing PQC algorithms in non-critical environments to test for performance, compatibility, and operational issues. Pilot programs should be used to gather feedback on the feasibility of large-scale deployment.

Phased rollout

A gradual implementation is key to a successful transition. Begin with low-impact systems and gradually move toward high-priority systems. This incremental approach allows for troubleshooting and optimisations throughout the process.

Hybrid cryptography

In the transition period, consider using hybrid solutions that combine classical and PQC algorithms. This provides a fallback in case of compatibility issues, allowing for a smoother transition while maintaining security.

Continuous monitoring and updates

As PQC standards and technologies evolve, it's essential to monitor advancements and update strategies accordingly. Organisations should also ensure compliance with new regulations and best practices.

The execution phase is about effectively operationalising the planned strategy. Organisations should consider:

Minimising downtime and disruption

Implement changes without affecting service availability. Carefully plan the migration timeline to minimise disruptions to business operations.

Ensuring ongoing security

Monitor and validate that all new cryptographic implementations are functioning as expected. Continuous monitoring is necessary to detect any issues early and ensure that the organisation remains quantum-resistant.

Migrating to PQC is a complex but necessary step to secure sensitive data against future quantum threats. The process of diagnosis, planning, and execution will not be straightforward. For example, adapting existing systems to PQC may encounter integration and performance issues, particularly with legacy systems. Moreover, organisations need to train their workforce on PQC concepts, standards, and the implementation process.

By proactively diagnosing current cryptographic assets, carefully planning a comprehensive migration strategy, and executing a phased rollout, organisations can ensure a smooth transition to quantum-safe cryptography.

The diagnosis should be started as soon as possible to lay the groundwork for a detailed and effective migration plan. Once planning is complete, a cautious but assertive execution ensures that sensitive systems remain protected as the quantum era approaches.

NCS-IBM partnership **Best-in-class technologies and services**

IBM's leadership in PQC

IBM has played a pivotal role in the development of PQC. As a major contributor to the NIST PQC standardisation process, IBM has demonstrated its commitment to quantum-safe technologies, collaborating with global experts to define algorithms that can resist quantum-based attacks. This early adoption of PQC highlights IBM's forward-thinking approach to cybersecurity and its ability to develop cutting-edge tools that address both current and future risks.

As quantum computing rapidly advances, traditional cryptographic systems are increasingly at risk of being rendered obsolete. IBM's proactive efforts in quantum-safe cryptography position it as a leader in providing technologies that ensure data remains secure, even in a post-quantum landscape.

NCS's Focus on Digital Resilience

NCS, on the other hand, focuses on securing digital transformations for clients across industries. As organisations undergo digital transformations, they face increasing cybersecurity risks, particularly as the digital landscape continues to evolve. NCS's comprehensive range of services—including professional services, technology integration, and managed services—helps clients navigate these risks, ensuring that their digital infrastructures are resilient against both current and emerging threats.

At the core of NCS's service offerings is its ability to provide end-to-end solutions. From strategy and planning to execution and monitoring, NCS ensures that clients can confidently pursue innovation and digital growth while maintaining security and compliance with local regulations.

Key value propositions of the NCS-IBM partnership

The NCS-IBM partnership combines expertise in Governance, Risk, and Compliance (GRC) with cutting-edge, quantum-safe technologies.

Augmentation to GRC services

NCS has deep expertise in GRC and a solid understanding of local cybersecurity regulations. By collaborating with IBM, NCS enhances its services with advanced quantum-safe cryptography. IBM's tools and algorithms, designed to combat post-quantum threats, help clients meet regulatory requirements while preparing for the future. This joint capability enables organisations across various sectors, including financial services, healthcare, and the public sector, to mitigate risks and safeguard their digital operations.

Innovation as a service

NCS's R&D capabilities, supported by its joint research lab with the National University of Singapore (NUS), provide a platform for testing and co-developing quantum-safe solutions. Together with IBM, NCS offers clients the opportunity to customise security solutions tailored to their unique needs. This collaborative innovation approach helps organisations address cybersecurity risks posed by quantum computing while future-proofing their operations.

Through strategic partnerships, such as the NCS-IBM collaboration, organisations can access best-in-class tools, services, and expertise to guide them through the transition to quantum-safe security.

Now is the time to act. Begin your journey to quantum-safe cryptography today by assessing your current vulnerabilities, developing a comprehensive migration strategy, and partnering with experts who can help you navigate the complexities of quantum-safe security.

nCS //



**Part 2: Automating
discovery of
cryptographic assets**



Introduction

In the modern digital era, organisations are tasked with managing and protecting vast amounts of sensitive data that require long-term retention. This data includes personal information, financial records, and intellectual property, all of which need protection with strong cryptographic technologies to ensure their security and integrity. However, the management of cryptographic assets, such as encryption keys and certificates, presents significant challenges, as these cryptographic assets must be discovered, managed accurately, and maintained in a timely and continuous manner.

Manual management of cryptographic assets can lead to increased risks of data breaches, non-compliance with regulations, and operational inefficiencies. According to the World Economic Forum, the proliferation of connected devices, such as IoT, is expected to reach more than 32 billion by 2030, representing a significant increase in attack surfaces for cyberattacks.¹

To address these issues, organisations can leverage automation and centralised management solutions such as those described in NIST SP 1800-38B.² Technologies such as automated discovery tools and centralised inventory management can enhance the security of sensitive data, ensure compliance with regulations, and improve overall operational efficiency.

By automating the discovery, identification, tracking, and management of cryptographic assets, organisations can mitigate the risks associated with manual processes and emerging threats, such as those posed by quantum computing. This proactive approach not only safeguards sensitive data but also supports the long-term success and resilience of the organisation.

Challenges faced by organisations in the management of cryptographic assets in the digital age

Organisations today face many challenges in managing cryptographic assets effectively and efficiently to ensure data security and compliance, such as:

- Regulatory pressure** Organisations are required to comply with stringent data protection regulations and standards, such as GDPR, HIPAA, and PCI DSS. These regulations mandate the secure handling, storage, and transmission of sensitive data, with severe penalties for non-compliance. Organisations often face regulatory pressure as they are required to implement data protection and security controls to safeguard sensitive data such as personal information, financial records, and intellectual property.
- Exponential growth of cryptographic assets** The volume and complexity of cryptographic assets, including encryption keys and digital certificates, have grown exponentially. This growth is driven by the increasing amount of data being generated and the need to secure it. Manual tracking and management of these assets has become impractical and error-prone, leading to potential security gaps and inefficiencies.
- Increased risks** The manual management of cryptographic assets can lead to increased risks of data breaches, non-compliance, and operational inefficiencies. Mismanagement of encryption keys and certificates can result in unauthorised access to sensitive data, data loss, and failure to meet regulatory requirements. These risks can have severe financial and reputational consequences for organisations.
- Emerging threats** The urgency for organisations to discover and manage their cryptographic assets has intensified due to emerging threats such as quantum computing. Quantum computing poses new vulnerabilities in cryptography, as it has the potential to break widely used encryption algorithms such as RSA and ECC algorithms mentioned in CNSA 2.0.³ Organisations must proactively identify and manage their cryptographic assets to mitigate these emerging threats and ensure the long-term security of their sensitive data.

By leveraging automation and centralised management solutions, organisations can enhance the security of their sensitive data, ensure compliance with regulations, and improve operational efficiency. These solutions enable the efficient discovery, tracking, and management of cryptographic assets, reducing the risks associated with manual processes and emerging threats.

Complexities in cryptographic asset management in a growing digital landscape

Organisations often face complexities associated with managing a large volume of cryptographic assets effectively, such as:

Scalability Issues

As organisations generate, transfer, and store increasing volumes of data to be protected, the number of cryptographic assets, such as encryption keys and certificates, also grows. This exponential increase complicates their management, making it difficult to maintain an accurate inventory and ensure that all data and cryptographic assets are properly secured and updated. Without scalable solutions, organisations struggle to keep up with the demands of managing and protecting these data and cryptographic assets effectively.

Human Error

Manual processes for managing cryptographic assets are inherently prone to human error. Mistakes in key generation, distribution, or revocation can lead to significant security vulnerabilities, such as unauthorised access to sensitive data or data breaches. These errors can undermine the integrity of cryptographic measures and expose organisations to substantial risks.

Regulatory Compliance

The landscape of data protection regulation is constantly evolving, with new standards and requirements being introduced regularly. Ensuring compliance with these regulations necessitates continuous monitoring and updating of security policies in managing cryptographic assets. Organisations must stay abreast of changes and implement necessary adjustments to avoid penalties and maintain the trust of their stakeholders.

Integration Challenges

Cryptographic assets are often dispersed across various systems, platforms, and applications within an organisation. This dispersion makes centralised management difficult, as it requires integrating disparate systems and ensuring consistent application of security policies in managing cryptographic assets. Without effective integration, organisations may face gaps in their security posture and struggle to comply with security policies and standards.

Merger and Acquisition

When organisations merge with or acquire other entities, the complexity of managing cryptographic assets increases significantly. Each organisation may have its own set of security policies, practices, tools, and assets, which need to be consolidated and harmonised. This process can be challenging and time-consuming, requiring careful planning and execution to ensure that all assets are accounted for and properly managed.

By addressing these complexities through automation and centralised management, organisations can enhance their ability to manage cryptographic assets at scale, reduce the risk of human error, ensure regulatory compliance, integrate disparate systems, and streamline asset management during mergers and acquisitions. This approach not only strengthens the security of sensitive data but also improves operational efficiency and resilience.

Enhancing cryptographic asset management: **Strategies for security and compliance**



Organisations should implement effective strategies for managing cryptographic assets to ensure security and compliance, such as:

Automated discovery tools

Implementing automated tools that can scan and identify cryptographic assets across the organisation is crucial. These tools reduce the reliance on manual processes, which are prone to errors and inefficiencies.

Automated discovery tools can quickly and accurately locate encryption keys, certificates, and other cryptographic assets, ensuring that no assets are overlooked. This comprehensive visibility allows organisations to maintain a complete inventory of their cryptographic assets, enhancing security and compliance.

Centralised management systems

Utilising centralised platforms to manage cryptographic assets ensures consistent application of security policies and simplifies compliance tracking. Centralised management systems provide a unified interface for handling encryption keys, certificates, and other cryptographic elements.

This approach streamlines operations, reduces the risk of mismanagement, and facilitates the enforcement of uniform security standards across the organisation. Centralised systems can integrate with existing IT infrastructure to provide seamless management and oversight.

Training and awareness

Educating staff on the importance of cryptographic asset management and best practices is vital to minimise human error. Training programs should cover the fundamentals of cryptography, the importance of proper key management, and the potential risks associated with improper key management.

By raising awareness and providing ongoing education, organisations can empower their employees to follow best practices and contribute to the overall security posture.

Regular audits and monitoring

Conducting regular audits and continuous monitoring is crucial for promptly detecting and addressing vulnerabilities. Regular audits help identify any discrepancies or weaknesses in the management of cryptographic assets, allowing organisations to take corrective actions before issues escalate.

Continuous monitoring ensures that any changes or anomalies in cryptographic practices are detected in real-time, enabling swift responses to potential threats. This proactive approach helps maintain the integrity and security of sensitive data.

By adopting these strategies, organisations can effectively manage and protect their cryptographic assets, ensuring the security and integrity of their sensitive data. This approach not only mitigates risks but also enhances operational efficiency and compliance with regulatory standards.

Figure 1 below illustrates the high-level architecture for automating the discovery of cryptographic assets.

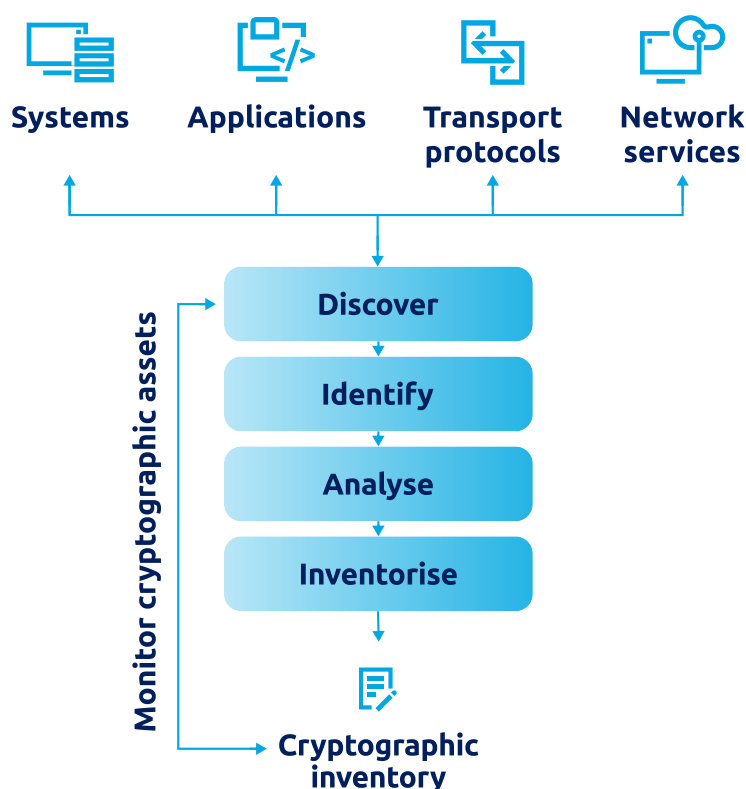


Figure 1: High-level architecture of an automated discovery of cryptographic assets.

Why NCS?

Cryptographic discovery solutions are still in their infancy and are unlikely to be fully automated. Therefore, organisations can benefit from the expertise and technical support of NCS. We can assist the organisations with the implementation and management of cryptographic solutions, offering guidance on best practices and helping to navigate complex regulatory requirements. With NCS, organisations can enhance their cryptographic capabilities and ensure the long-term security of their sensitive data.

NCS possesses the necessary skills, resources, and capabilities to address quantum-safe security and further advance quantum-safe security solutions in the industry. These include:

- A suite of professional services leveraging the expertise of NCS and partners in areas such as compliance and risk management.
- A team of qualified and certified cyber professionals with unique domain knowledge in IT, OT, IoT and 5G security.
- Strong research capabilities and close collaboration with NUS and leading vendors in cybersecurity.

Conclusion

In conclusion, the management and protection of cryptographic assets are crucial for organisations that handle large volumes of sensitive data with extended retention periods. The complications arising from scalability issues, human error, regulatory compliance, integration challenges, and mergers and acquisitions necessitate a robust approach to managing cryptographic assets.

By implementing automated discovery tools, centralised management systems, regular audits and monitoring, comprehensive training programs, and leveraging external expertise, organisations can significantly enhance their security posture. These measures ensure the integrity and confidentiality of sensitive data, facilitate compliance with evolving regulations, and improve operational efficiency. Ultimately, adopting these strategies enables organisations to navigate the complexities of cryptographic asset management and safeguard their valuable data against emerging threats.

nCS //



Part 3: Security validation of Quantum Key Distribution Networks



Introduction

The rapid advancement in quantum computing poses a significant threat to break public-key systems used to distribute encryption keys, which are essential for data protection and secure communication. This means sensitive data in organisations is now at risk of being compromised due to these potential threats from quantum computing. In 2024, MAS issued an advisory to all financial institutions on cybersecurity risks associated with quantum technology, providing recommendations to safeguard against such threats.¹

Quantum Key Distribution (QKD) networks (QKDN) offer a promising solution to safeguard sensitive data against such threats by using the principles of quantum mechanics to distribute encryption keys securely. QKDN uses truly random shared keys to achieve information-theoretic security against any form of eavesdropping, including those from quantum computing. In 2023, IMDA released the reference specification to provide a guideline for organisations to deploy QKDN.² Many organisations have also started conducting pilot projects to validate QKDN in real-world scenarios. For instance, MAS is collaborating with banks and technology partners to study the application of QKDN in financial services.³

Deploying QKDN in real-world applications presents several challenges. Firstly, QKDN requires domain knowledge in quantum physics, cybersecurity, and engineering. However, most QKDN developers lack cybersecurity and engineering knowledge. This adds complexity and vulnerabilities to QKDN deployment and integration with cryptographic applications. Cybersecurity teams also need multi-disciplinary knowledge to develop and conduct security validation on QKDN. Secondly, integrating QKDN with cryptographic applications does not guarantee quantum safety.

A long lead time is required to deploy and integrate QKDN securely with cryptographic applications before security validation can be carried out. Lastly, while there are established standards in the design and implementation of QKDN, there are minimal established standards or guidelines for conducting security validation of QKDN integrated with cryptographic applications. For instance, ITU-T provides the security framework for QKDN, which covers QKDN and its connections to the user network only.⁴

To address these challenges, NCS collaborated with a government agency to conduct a study on validating the quantum-safe security of an organisation that utilises QKDN. NCS developed the QKDN security validation as follows:

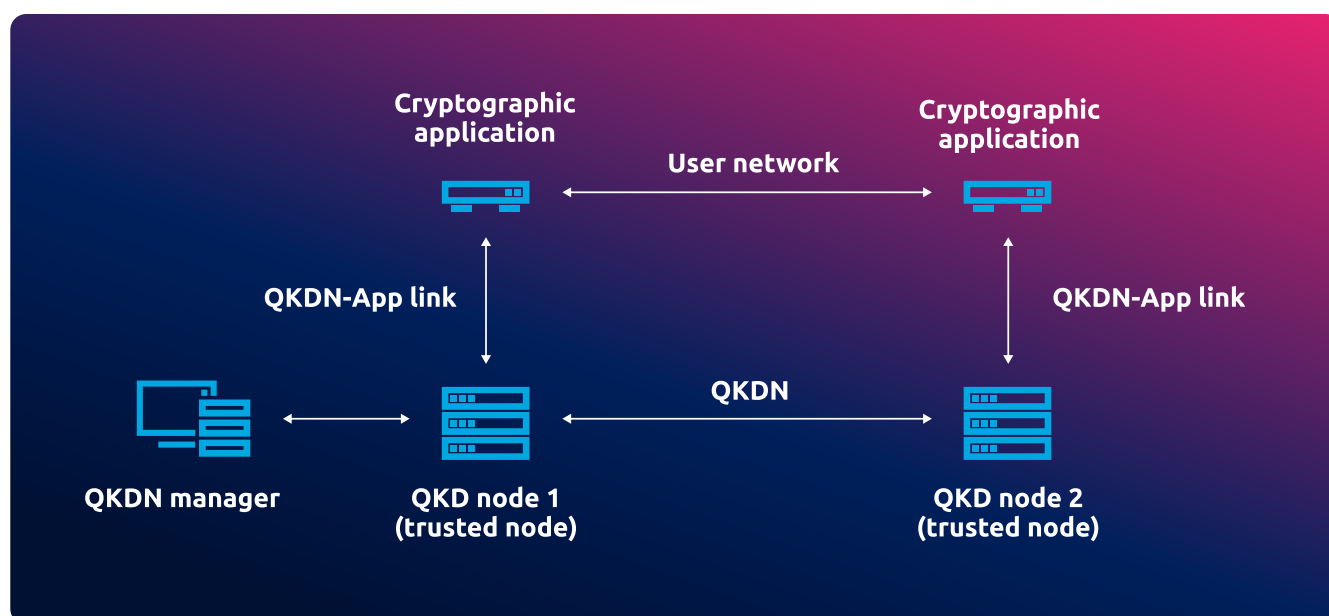
- | | | |
|--|---|--|
| 1
Identify suitable test cases to develop and validate the security of the QKDN. | 2
Conduct compliance checks on QKDN against established standards such as ITU-T and ETSI. | 3
Analyse the impact on Confidentiality, Integrity and Availability of QKDN. |
|--|---|--|

Identification of suitable test cases

The proposed test cases in the study were selected based on the security aspect of QKDN. These test cases are as follows:

1. QKD key randomness
2. Authentication and access control
3. Key management
4. Integration with cryptographic applications

The diagram below illustrates the setup of a small-scale QKDN used for conducting security validation based on various test cases.



The QKDN manager is responsible for the overall management of the QKDN. The QKD node contains the QKD module in a trusted node which is secure against intrusion and attacks. The QKDN comprises the QKD link, the key management link, the control link, and the management link. Within the QKD link are the quantum and service channels, which are responsible for generating QKD keys. The cryptographic applications are integrated with the QKDN to receive QKD keys via the QKDN-App links, establishing a secure user network.

Test case #1

QKD key randomness

In QKDN, perfect randomness is crucial for secure key generation. Any deviation from this ideal randomness will weaken the security of the exchanged keys. QKDN rely on the quantum key random generator to produce truly random numbers for key generation.

To test for the randomness of the keys generated by QKDN, a set of statistical tools based on NIST SP 800-22 was used.⁵ A Get Key command was used to retrieve the keys from the QKDN via the QKDN manager.⁶ At least 1 million bits were collected by executing the Get Key command continuously and concatenating the keys together as one long string of bits. If the p-values from the statistical tests are high, this proves that the QKD keys are genuinely random.

Test case #2

Authentication and access control

Validating authentication in QKDN is crucial to ensure that the key distribution process is secure from unauthorised access and that the identities of the communicating parties are correctly verified. The authentication process in QKDN involves verifying that the parties involved in the communication are who they claim to be. The effectiveness of access control to the QKDN ensures that only authorised entities can access QKD keys and their derived cryptographic keys, if any.

QKD modules and cryptographic applications typically use certificates issued by a QKDN manager to authenticate each other before exchanging keys.⁷ In this case, a spoofing attack using a forged certificate issued by the QKDN manager to one of the QKD modules can be simulated to validate if the compromised QKD module with the forged certificate can successfully authenticate with the other QKD module and the connected cryptographic application. If the authentication by the compromised QKD module fails, it means that the QKDN is secure against spoofing attacks.

Test case #3

Key management

Ensuring proper key management in QKDN requires a focus on both the unique aspects of QKD keys and the integration with existing key management practices. The focus is on secure key lifecycle management to ensure the confidentiality, integrity and availability of QKD keys throughout their lifecycle.

For example, to test the availability of QKD keys, a Denial-of-Service (DoS) attack can be simulated in the QKDN to determine if cryptographic applications can still request QKD keys under such an attack. This can be achieved using security testing tools such as Hping3 and Ettercap to simulate a high volume of traffic within the QKDN, or by utilising QKDN commands like Get Key to consume the keys quickly.

Test case #4

Integration with cryptographic applications

Integration of QKDN with cryptographic applications to protect critical applications against quantum threats is non-trivial and requires a thorough assessment of the combined security measures, ensuring that the integration does not compromise the security enhancements offered by QKD against quantum threats. The focus is on interoperability and end-to-end security analysis to validate if the confidentiality and integrity of sensitive data can be preserved without introducing vulnerabilities that could lead to a regression in security.

For instance, it is required for the QKDN-App links to use HTTPS protocols with TLS 1.2 or higher.⁸ However, some cipher suites used in TLS 1.2 can be vulnerable, such as the AES-CBC mode, which is vulnerable to padding oracle attacks.⁷ Cryptographic applications should also be checked for known vulnerabilities using well-known sources such as Common Vulnerabilities and Exposures (CVE), Known Exploited Vulnerabilities (KEV) and Common Weakness Enumeration (CWE).

NCS strategy for QKDN security validation

NCS possesses the necessary skills, resources, and capabilities to provide security validation of QKDN and advance quantum-safe solutions in the industry. These include:

- A suite of quantum-safe security services and consultancy leveraging on the expertise of NCS and partners in areas such as compliance and risk management.
- A team of qualified and certified cyber professionals with unique domain knowledge in IT, OT, IoT, 5G, and quantum-safe security.
- Strong research capabilities and close collaboration with NUS and leading vendors in cybersecurity.

NCS can help enterprises build their awareness and expertise in QKDN and other quantum-safe security technologies through the conduct of small-scale projects in real-world scenarios and regular quantum-safe security workshops, keeping them updated on the latest developments in quantum technologies.

Conclusion

The proposed security validation guideline for QKDN will provide a systematic approach to guide enterprises to deploy, implement, and integrate QKDN securely with their cryptographic applications and systems. NCS can tailor the quantum-safe security validation requirement to meet the operational and security needs of enterprises.

Summary

From strategy to action

Preparing for a quantum-safe future is not a single initiative; it is a journey. This guide has shown that readiness requires three interconnected steps:

- Setting a strategic direction with a clear migration roadmap.
- Establishing practical foundations through automated discovery of cryptographic assets.
- Building confidence and trust by validating advanced technologies such as Quantum Key Distribution Networks (QKDNs).

Why timing matters

The shift to post-quantum cryptography (PQC) is inevitable. The question is not if, but when. Organisations that begin now can spread investment over time, reduce the risk of rushed last-minute projects, and demonstrate resilience to customers, partners, and regulators. Those who wait may find themselves caught in a costly scramble.

The role of NCS

As this guide highlights, NCS is uniquely positioned to support organisations across every stage of the journey. From shaping strategy to deploying automation tools and conducting rigorous technical validation, NCS provides both the breadth and depth of expertise required for a successful transition.

Final word

Quantum disruption will redefine the security landscape. However, with the right plan, discovery processes, and validation measures in place, it can also become an opportunity to lead with resilience, inspire confidence, and turn uncertainty into an advantage.

The time to act is **now**.



Contact us

References

About the sources

The references included in this publication were drawn from trusted, publicly available materials issued by recognised global standards bodies, cybersecurity agencies, and research organisations.

Part 1 – Preparing for a Quantum-Safe Future

[1] Ceci, L. (2024, August 27). Number of unique WhatsApp mobile users worldwide from January 2020 to June 2024. Statista.

https://info.idc.com/rs/081-ATC-910/images/US-IDC-FutureScape-2025-GenAI_ebook.pdf

[2] Google. (2024). Transparency report: HTTPS encryption on the web. Google Transparency Report.

<https://transparencyreport.google.com/https/overview>

[3] Neskey, C. (2024, October 9). Are your passwords in the green? Hive Systems.

<https://www.hivesystems.com/blog/are-your-passwords-in-the-green>

Part 2 – Automating Discovery of Cryptographic Assets

[1] World Economic Forum. (2024, October). Navigating cyber resilience in the age of emerging technologies: Collaborative solutions for complex challenges. World Economic Forum.

[2] National Institute of Standards and Technology. (2023, December). NIST Special Publication 1800-38B: Migration to post-quantum cryptography – Quantum readiness: Cryptographic discovery Volume B: Approach, architecture, and security characteristics of public key application discovery tools. U.S. Department of Commerce.

[3] National Security Agency. (2024, April). The Commercial National Security Algorithm Suite 2.0 and quantum computing FAQ. National Security Agency.

Part 3 – Security Validation of Quantum Key Distribution Networks

[1] European Telecommunications Standards Institute. (2019, February). GS QKD 014: Quantum key distribution (QKD); Protocol and data format of REST-based key delivery API. ETSI.

[2] Infocomm Media Development Authority. (2023, June). Reference specification: Quantum key distribution networks (IMDA RS QKDN Issue 1). IMDA.

[3] International Telecommunication Union. (2020, October). X.1710: Security framework for quantum key distribution networks. ITU-T.

[4] International Telecommunication Union. (2023, November). Y.3804 (2020) Quantum key distribution networks – Control and management (Amendment 1). ITU-T.

[5] Monetary Authority of Singapore. (2024, February 20). Advisory on addressing the cybersecurity risks associated with quantum (Circular No. MAS/TCRS/2024/01). MAS.

[6] Monetary Authority of Singapore. (2024, March 20). MAS collaborates with banks and technology partners on quantum security. MAS.

<https://www.mas.gov.sg/news/media-releases/2024/mas-collaborates-with-banks-and-technology-partners-on-quantum-security>

[7] Microsoft. (2025, March 21). CBC decryption vulnerability – .NET. Microsoft Learn.

<https://learn.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode>

[8] National Institute of Standards and Technology. (2010, April). SP 800-22 Revision 1a: A statistical test suite for random and pseudorandom number generators for cryptographic applications. U.S. Department of Commerce.