Key Elements of PQC and Readiness

Key Elements of Post-Quantum Cryptography (PQC) and Readiness

As quantum computing technology continues to evolve, the security of Public Key Infrastructures (PKI) will face new challenges. Quantum computers have the potential to break widely used cryptographic algorithms like RSA and ECC, which form the backbone of modern PKI systems. Preparing for the transition to Post-Quantum Cryptography (PQC) is crucial to maintain the integrity and security of digital certificates and cryptographic services in a quantum future.

Here's a guide on PQC and being ready for quantum computing:

1. Why Quantum Computing Threatens PKI

Understanding the Quantum Threat

- **Quantum Computers and Cryptography:** Quantum computers, once fully developed, will be able to solve mathematical problems much faster than classical computers. Shor's algorithm, in particular, can factor large numbers efficiently, rendering RSA and ECC (widely used in PKI) vulnerable to quantum attacks.
- **Impact on PKI:** PKI systems that rely on RSA, ECC, or similar public-key algorithms will be at risk of being broken by quantum computers. This could allow attackers to forge digital signatures, impersonate users, or decrypt sensitive information.

Key Message: PKI customers must understand that their current cryptographic security could become obsolete with the advent of quantum computing and should begin preparing now for the transition to quantum-safe solutions.

2. The Timeline for Quantum Computing and PQC

Quantum Computing Readiness

- **Quantum Threat Horizon:** While large-scale quantum computers capable of breaking RSA and ECC are not expected to emerge for several years, it's important to prepare in advance. The process of transitioning to quantum-safe cryptography can take time, and there may be a period of overlap between classical and quantum-safe cryptographic systems.

Post-Quantum Cryptography Standardisation:

- **NIST PQC Project**: The National Institute of Standards and Technology (NIST) has been leading efforts to identify and standardise post-quantum cryptographic algorithms. NIST is expected to release finalised standards in the coming years, and PKI customers should plan for a future migration.

Key Message: While quantum computers may still be a decade away, the time to start planning for post-quantum cryptography is now. Customers should monitor developments in PQC and prepare to adopt new standards when they become available.

3. Post-Quantum Cryptography (PQC) Explained

What is PQC?

- **Quantum-Resistant Algorithms:** Post-Quantum Cryptography refers to cryptographic algorithms that are believed to be resistant to attacks by quantum computers. These algorithms are designed to replace vulnerable public-key algorithms like RSA and ECC in PKI systems.
- **Algorithms Under Consideration:** Some of the leading candidates for PQC include lattice-based cryptography, hash-based signatures, multivariate equations, and code-based cryptography. Each has its strengths and weaknesses in terms of performance, security, and compatibility with existing systems.

Key Message: PQC will ensure the security of cryptographic systems in the quantum era. PKI customers should become familiar with the emerging PQC algorithms and assess which ones may be best suited for their environments once they are standardised.

4. Transition to Quantum-Safe PKI

Hybrid Approaches

- **Combining Classical and PQC:** As PQC standards evolve, PKI systems may need to adopt hybrid approaches, combining traditional cryptographic algorithms with quantum-safe ones. This allows for a smoother transition while maintaining security in the face of both classical and quantum threats.

Cryptographic Agility

- **Flexible Systems:** Ensure your PKI system is cryptographically agile, meaning it can quickly adapt to new cryptographic algorithms without requiring a complete overhaul. Cryptographic agility will be essential for transitioning to PQC algorithms once they are standardised.

Key Message: PKI customers should plan for a phased migration to PQC by adopting hybrid approaches and ensuring their systems are cryptographically agile. This allows them to remain secure during the transition to quantum-safe cryptography.

5. Secure Long-Lived Data

Data Harvesting Risks

- **"Harvest Now, Decrypt Later" Attacks**: Some attackers may be intercepting and storing encrypted data today, with the intention of decrypting it later using quantum computers. This poses a significant risk for data that must remain confidential over the long term (e.g. financial records, healthcare information, and government communications).
- **Long-Term Encryption Solutions:** To mitigate this risk, PKI customers should begin encrypting long-lived data using quantum-safe algorithms sooner rather than later. By doing so, they ensure that their sensitive data remains secure even when quantum computers become a reality.

Key Message: PKI customers with sensitive, long-lived data should begin using PQC for encryption now to protect against future quantum attacks. Waiting too long could expose valuable data to quantum threats.

6. Key Management in a Quantum World

Post-Quantum Key Management

- **Key Generation and Distribution:** Quantum-safe cryptography will require new approaches to key management. PKI customers need to be prepared for changes in how cryptographic keys are generated, distributed, and stored.
- **Hardware Security Modules (HSMs):** Ensure that the Hardware Security Modules (HSMs) used for key management are compatible with post-quantum algorithms and can store and handle larger keys that may be required by PQC.

Key Message: PKI customers should assess their key management systems to ensure they can support post-quantum cryptographic keys. Future-proofing key management systems now will make the transition to PQC smoother.

7. Industry Regulations and Compliance

Regulatory Considerations

- **Compliance with New Standards:** As PQC standards are developed, industry regulations and compliance requirements will evolve. PKI customers in regulated industries (e.g. finance, healthcare, government) must stay informed about these changes and ensure they remain compliant as cryptographic standards shift.
- **Proactive Audits:** Start conducting proactive cryptographic audits to identify vulnerabilities in current systems and prepare for compliance with future quantum-safe requirements.

Key Message: PKI customers in regulated industries should stay ahead of regulatory changes related to quantum-safe cryptography and ensure their systems will comply with future PQC standards.

8. Collaboration with Vendors and Partners

Partnering for Quantum Readiness

- **Support:** Work closely with PKI vendos, like Cogito, to ensure that they have a roadmap for supporting PQC. Regularly engage with your vendors to discuss their PQC strategy and ensure they are planning for quantum-safe transitions.
- **Collaborating on Best Practices:** Share insights and best practices with industry peers and partners to develop a cohesive approach to quantum readiness. Collaborate on efforts to adopt PQC and standardise best practices across industries.

Key Message: PKI customers should engage with vendors and partners, like Cogito Group to ensure they are collectively preparing for the transition to quantum-safe cryptography. Collaboration will be key to ensuring a smooth and secure migration to PQC.

Conclusion: The Path to Quantum Readiness

Preparing for a post-quantum world is not a distant concern—it is a present-day priority for organisations relying on PKI for security. By understanding the quantum threat landscape, staying informed on PQC developments, and taking proactive steps to secure long-lived data and implement cryptographic agility, PKI customers can ensure their systems remain resilient against future quantum threats.

Key Takeaway for Customers: Start planning your quantum readiness roadmap now. Collaborate with Cogito Group, assess your current cryptographic infrastructure, and be prepared to transition to post-quantum cryptography to safeguard your organisation in the quantum era.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.