TYTO Athene

ADDRESSING QUANTUM COMPUTING THREATS

As quantum computing advances, traditional encryption methods face increasing risk. Quantum computers have the potential to decrypt data previously considered secure, posing a significant threat to sensitive government information. In response, the Secretary of Commerce has approved three Federal Information Processing Standards (FIPS) for post-quantum cryptography: FIPS 203, 204, and 205.

Highlights

Post-Quantum Cryptography (PQC) is the next frontier in cybersecurity, protecting your organization from the imminent threats posed by quantum computing. Tyto Athene offers a comprehensive PQC service designed to secure your systems against both quantum and conventional attacks, ensuring long-term data integrity and compliance with evolving national security standards.

Moving to PQC requires compatibility and interoperability with existing systems, many of which are legacy systems in government and enterprise organizations.

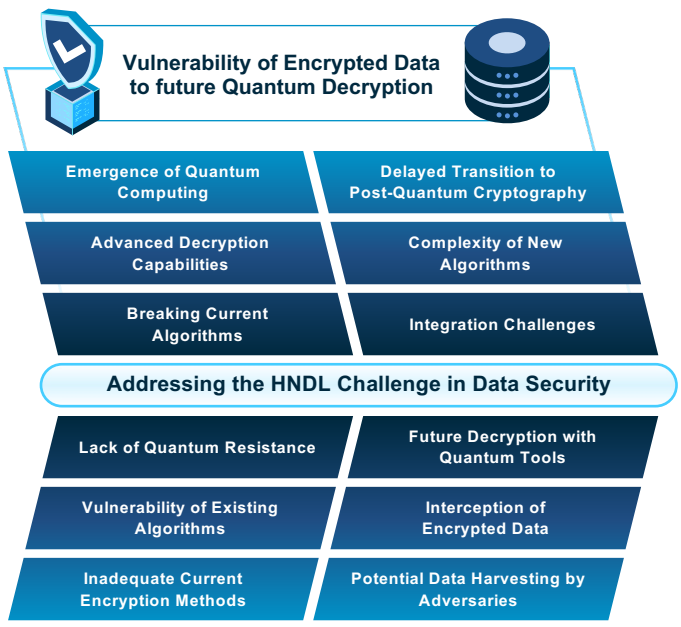
Rapid changes in cryptographic standards complicate decision-making.

From software updates to staff training, the costs can be substantial, particularly for large-scale government or enterprise organizations that need widespread adoption across all systems.

The shift to PQC demands skilled personnel with expertise in quantum computing and advanced cryptography. Existing IT staff often need extensive retraining to handle the new algorithms and understand PQC's implications on system design and risk management. Organizations also face challenges in establishing a centralized encryption policy and ensuring compliance, especially within departments where roles and responsibilities differ significantly.

Key Benefits of Quantum-Resistant Security

- **Enhanced Protection for Government and Sensitive Data**
  Safeguards critical information from quantum decryption threats, ensuring secure data storage and communication for years to come.
- **Compliance with Industry Standards**
  Meets Federal Information Processing Standards (FIPS 203, 204, and 205), enabling trusted, government-grade security.
- **Future-Proof Encryption**
  Provides robust data security to address both current and future advancements in quantum computing.
- **Minimal Operational Disruption**
  Phased integration approach ensures that PQC implementation fits seamlessly with existing systems, reducing impact on daily operations.
- **Comprehensive Support and Training**
  Empowers internal teams with the knowledge and skills necessary to manage post-quantum cryptography securely and effectively.



PQC BOM Builder App

Tyto Athene has developed current tools to validate the current state of TLS 1.3 deployment to predict interim safety of your existing services.

Ongoing development to build an automation scanning tool that will survey customer environments to assemble a BoM for existing encryption hardware and software. It will also help assess the hygiene of the PKI infrastructure.

Understanding The Challenge of Quantum Computing

Quantum computing leverages the principles of superposition and entanglement, allowing quantum bits (qubits) to exist in multiple states simultaneously. This enables quantum computers to perform complex calculations at unprecedented speeds, reducing tasks that would take years to mere hours. This processing power threatens the effectiveness of traditional encryption algorithms like AES, rendering them vulnerable. Implementing quantum-resistant encryption algorithms, such as those being standardized by NIST, is essential to defend against these emerging decryption capabilities.

The Threat of "harvest now, decrypt later"

Sensitive data, including classified information, medical records, and proprietary business data, requires long-term protection. Adversaries can employ a "harvest now, decrypt later" strategy—intercepting encrypted data today with the intent to decrypt it with future quantum technology. Government agencies and organizations handling sensitive data must act now to safeguard data integrity and security against these evolving quantum threats.

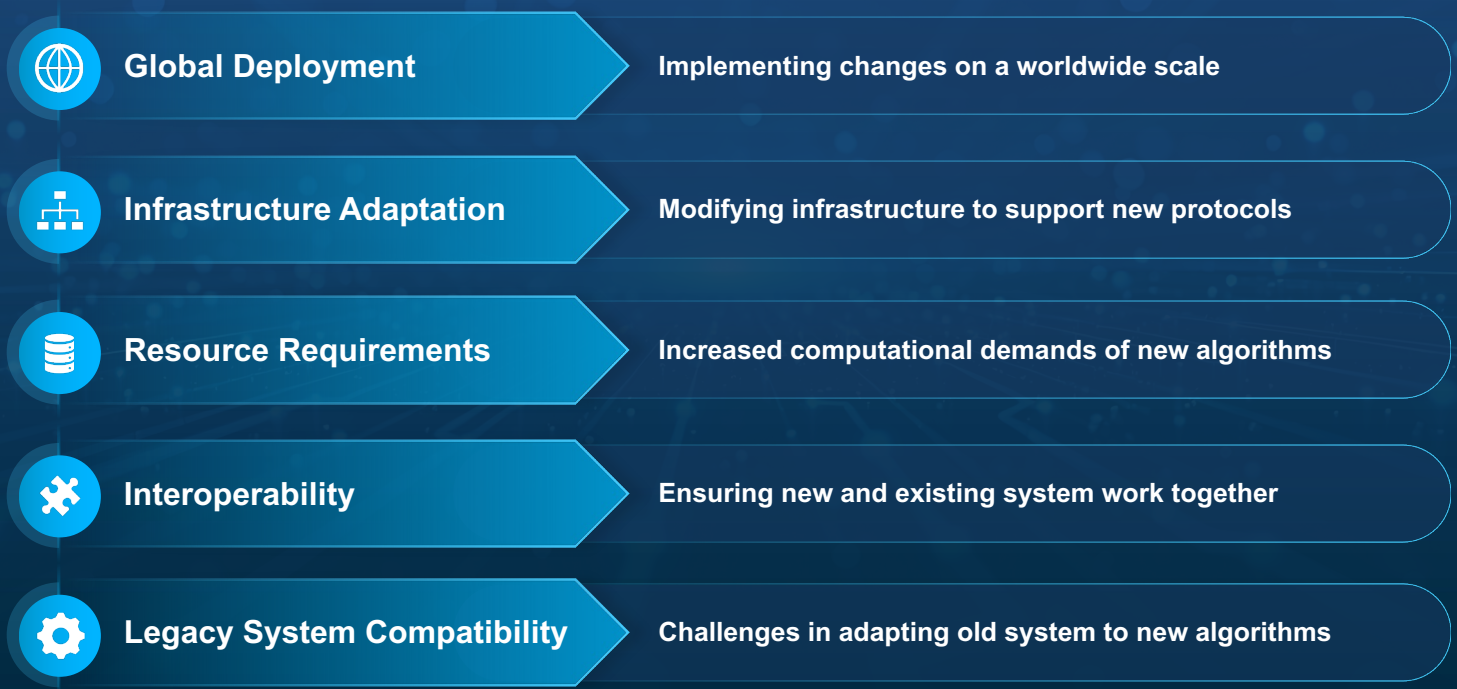
Challenges in Implementing Post-Quantum Cryptography (PQC)

Transitioning to PQC in large government environments involves several critical challenges:

- **Technical**: Ensuring compatibility, integration, performance, and scalability.
- **Business**: Addressing security risk management, cost considerations, compliance, and standardization.
- **Financial**: PQC migration is resource-intensive, requiring substantial investment.
- **Cultural and Human Resources**: Addressing training and skill gaps among personnel.

Successful PQC adoption requires a well-planned approach that extends beyond technology integration, involving strategic alignment across departments and balancing operational demands with new security requirements.

Challenges in Navigating Post-Quantum Cryptography (PQC)



The Solution: Post-Quantum Cryptography (PQC)

Integrating PQC is crucial to mitigate quantum threats. PQC solutions are designed to secure data against both quantum and classical computing risks, providing future-proofed encryption as quantum technology continues to evolve.

Future-Proof Security

Safeguard your data from quantum computing threats before they emerge. PQC is designed to withstand attacks from both conventional and quantum computers.

National Standards Compliance

Align with the latest directives from NIST and the White House's National Security Memorandum 10, ensuring your agency meets upcoming federal requirements.

Seamless, Tailored Integration

Our team of experts follow a customized transition plan tailored to your agency's unique needs and mission to ensure your PQC solutions integrate with existing systems, minimizing disruption and maintaining operational efficiency.

Tyto Athene's Approach to PQC Implementation

Quantum Encryption Readiness Assessment

- Evaluate current systems to identify vulnerabilities.
- Conduct threat analysis and inventory resources.
- Prioritize high-risk systems with a multi-faceted scoring system.

Algorithm Impact Assessment & Performance Testing

- Select and test NIST-endorsed PQC algorithms.
- Align business risk profiles with data sensitivity needs.
- Validate performance to ensure a seamless user experience.

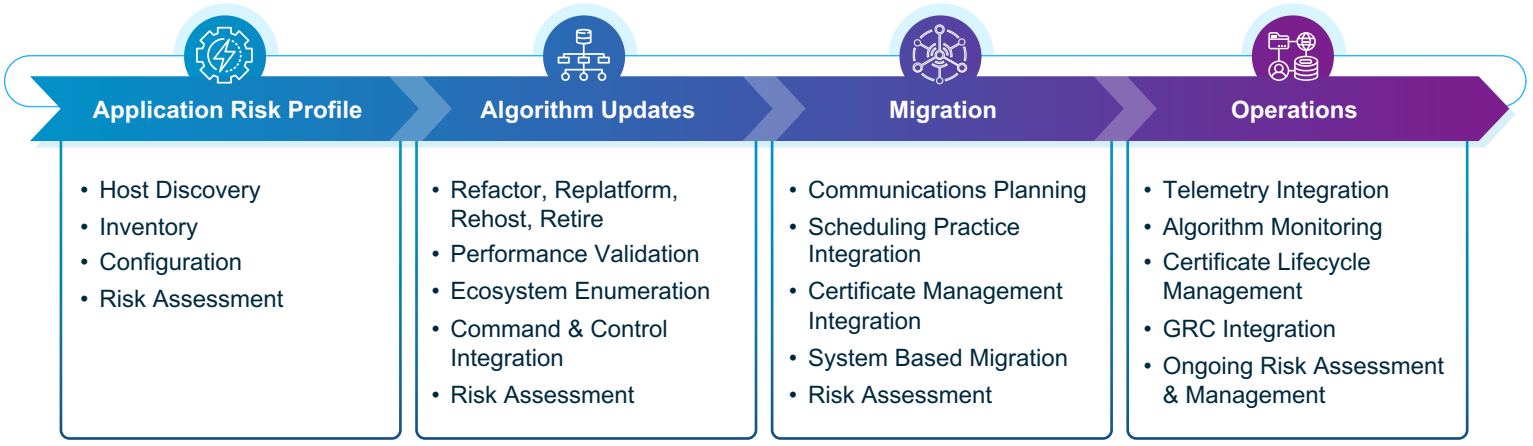
Seamless Migration & Integration

- Implement a phased migration strategy.
- Integrate PQC with DevSecOps pipelines.
- Train support staff to enable cross-team collaboration.

Ongoing Operations & Support

- Continuous monitoring and threat intelligence updates.
- Ensure compliance with NIST and global data protection regulations.
- Maintain scalability and performance of PQC systems.

Crypto Agility



Why Tyto Athene

With a proven track record in cybersecurity, Tyto Athene is uniquely positioned to guide organizations in transitioning to post-quantum cryptography. Through tailored roadmaps, expert project management, and end-to-end engineering solutions, Tyto Athene helps secure critical data and systems for the future.

1,700+
EMPLOYEES WITH
OVER 300
CERTIFICATIONS

85%
SECRET OR ABOVE SECURITY CLEARANCE

ML3 CMMI APPRAISED SVC SPM
ISO 9001 2015 CERTIFIED
TRUSTED CSfC INTEGRATOR
FR FedRAMP
SOC 2 AUDITED TYPE I

Future-Proof Data Security & Organizational Benefits

Tyto Athene's PQC strategy prepares organizations for both immediate and long-term cryptographic threats posed by quantum advancements.

Agility in Encryption:
Centralized policy management allows for updates as encryption standards evolve without full system overhauls.

Future-Proof Critical Systems:
Structured roadmap enables phased updates, keeping critical systems secure as PQC and regulatory needs advance.

Comprehensive Training and Knowledge:
Tyto Athene's training programs ensure internal teams are proficient in managing PQC, sustaining high security across the organization.

Our cryptographic and systems integration experts, along with industry leading vendors specializing in post-quantum encryption, are here to guide you through the selection and implementation phases. Migrating to PQC is crucial and demands a multi-year, multi-faceted approach to meet PQC requirements, such as M-23-02, and to protect your enterprise's digital assets from future quantum threats. Partnering with Tyto Athene and following our structured approach will ensure a seamless transition and uphold the highest standards of data security.

For more information about our cybersecurity services, please email bd@gotyto.com

https://gotyto.com

Tyto GSI is registered in System for Award Management (SAM) as a Large Business under NAICS Code 541519.

TYTO Athene
DATA TO DOMINANCE