White Paper



Best Practices for Implementing Quantum Resistant Security

thalestct.com

THALES
Building a future we can all trust

THALES

The arrival of large-scale, cryptographically relevant quantum computers is no longer a distant theoretical concern—it is now a planning-level reality. Although experts still debate the exact timeline, government and industry agree on one point: the threat to today's cryptographic systems is already active. Adversaries are believed to be collecting encrypted data now with the intent to decrypt it later, once quantum capabilities mature. This "Harvest Now, Decrypt Later" (HNDL) threat has elevated the transition to Post-Quantum Cryptography (PQC) from a future initiative to an immediate national priority.

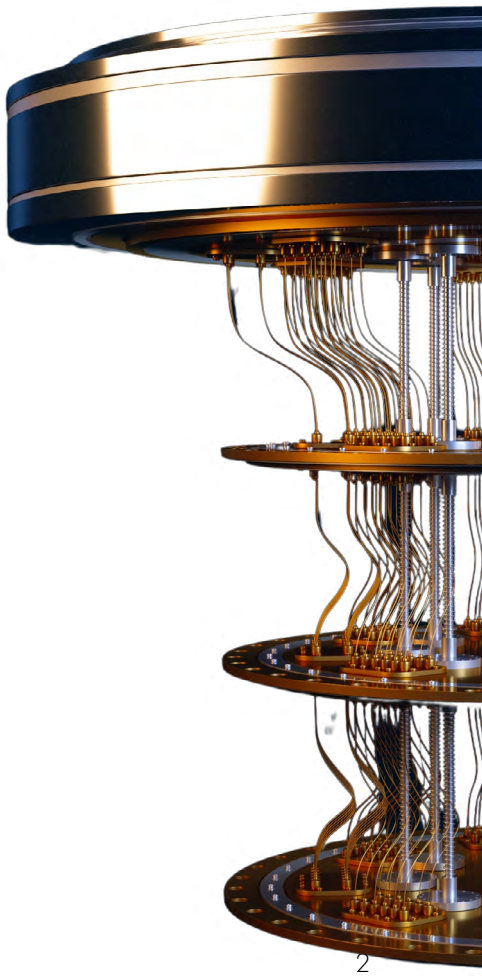
The Cloud Security Alliance estimates that quantum systems capable of breaking widely deployed Public Key Infrastructure (PKI) could emerge as early as 2030. Whether quantum advantage arrives in 2029, 2035, or later, U.S. Federal agencies cannot afford to wait for certainty. Sensitive, long-lived data—intelligence, mission information, operational technology, critical infrastructure controls, and citizen records—must be protected well before quantum computers become operational.

The Federal Government has been preparing for this shift for years. National Security Memorandum 10 (NSM-10), issued in May 2022, established clear requirements for transitioning to quantum-resistant cryptography and directed agencies to begin immediate preparation. The June 2026 release of Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," expanded that mandate. EO 14412 is a government-wide call to action for the most significant cryptographic migration in modern history. It accelerates adoption of PQC across federal systems and critical infrastructure, establishes new compliance obligations for federal contractors, mandates agency PQC Migration Leads, and sets firm deadlines for replacing vulnerable key-establishment and digital signature mechanisms.

The message is clear: agencies must act now. Mapping cryptographic assets, adopting crypto-agile architectures, and initiating phased migration to PQC are essential steps to ensure that federal systems and data remain secure in the quantum era.

Which Quantum?

As organizations prepare for the coming impact of quantum technologies, it's important to recognize that "quantum" is not a single concept but a broad category encompassing several distinct innovations. Each technology interacts with cybersecurity in different ways—some introduce new risks, while others offer powerful opportunities to strengthen protection. The following overview clarifies the major quantum-related technologies and their security implications, helping leaders understand what each does, how it works, and why it matters.



Quantum Computing

Quantum computers leverage the principles of quantum mechanics to perform certain mathematical operations exponentially faster than classical computers. Instead of traditional binary bits, they use qubits, which can represent multiple states simultaneously due to superposition and entanglement. A sufficiently powerful quantum computer could solve specific problems—such as factoring large numbers—far beyond the reach of classical systems, posing significant risks to today's cryptographic algorithms.

Quantum Key Distribution (QKD)

Quantum key distribution is a specialized cryptographic technique that uses quantum physics—not mathematics—to securely distribute symmetric keys between parties. QKD hardware transmits quantum states (usually photons) that cannot be measured or intercepted without detection, providing strong protections against eavesdropping. However, QKD only distributes keys; it does not replace encryption algorithms and must be integrated into a broader cryptographic system to be effective.

THALES

Quantum Random Number Generators (QRNG)

QRNGs generate nondeterministic random numbers by capturing inherent quantum effects. Typical QRNG chips contain a light-emitting diode (LED) and a sensor that counts photons emitted from the LED. Because quantum noise causes the number of emitted photons to vary unpredictably, QRNGs produce high-quality randomness—useful for security applications such as key generation, entropy sources, and hardware security modules.

Post-Quantum Cryptography (PQC)

Also known as quantum-resistant cryptography, PQC refers to algorithms designed to remain secure against both classical and quantum computers. PQC systems are implemented in software and hardware and are designed to interoperate with existing networks, protocols, and infrastructure, enabling organizations to migrate to quantum-safe protection without abandoning traditional architectures.

Migration to Post-Quantum Cryptography Guidance

The Federal Government has issued several complementary directives and guidance documents to support agencies as they prepare for the transition to post-quantum cryptography dating back to at least 2022 with NSM-10. Collectively, this body of guidance provides agencies with a clear roadmap for planning, testing, and executing a secure and timely transition to PQC.

Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks (June 2026). Executive Order 14412 directs the Federal Government to accelerate its transition to post-quantum cryptography to protect national systems from future quantum-enabled cyber threats. It requires each agency to designate a PQC Migration Lead within 30 days (July 2026) and, within 90 days, to follow forthcoming guidance from OMB, CISA, and the National Cyber Director. Agencies must review their High Value Assets and High Impact Systems and create plans to migrate those systems to NIST-approved quantum-safe algorithms—specifically implementing PQC for key establishment by December 31, 2030, and for digital signatures by December 31, 2031.

M-26-15: Execution of the Migration to Post-Quantum Cryptography (June 2026) The Office of Management and Budget's (OMB) directive accelerates the federal transition to PQC by requiring every civilian agency to designate a PQC Migration Lead and submit a detailed migration plan within 120 days, outlining how they will protect sensitive data from future quantum decryption threats. It establishes a five-phase timeline running from 2026 to 2035 that moves agencies from strategy and asset discovery through pilots, early migration, and transitions of key establishment and digital signatures, culminating in full PQC adoption. Agencies must use NIST-approved algorithms, employ hybrid and crypto-agile architectures, and maintain automated Cryptographic Bills of Materials (CBOMs) for continuous inventory. The mandate also extends PQC requirements to contractors by 2030, strengthening national cybersecurity resilience and reinforcing U.S. leadership in quantum-safe technology.

Additional PQC Guidance

The following federal directives and resources further outline the foundations, requirements, and guidance shaping the government's transition to post quantum cryptography:

NIST IR 8547: Transition to Post-Quantum Cryptography Standards (October 2026): Transition to Post-Quantum Cryptographic Standards

Executive Order 14413 (June 2026) The next frontier in quantum innovation

GSA Post Quantum Cryptography Buyer's Guide (June 2025): PQC procurement guidance

Department of War PQC Memo (Nov 2025) Preparing for migration to PQC

Whitehouse OMB M-24-14 Administration Cybersecurity Priorities for the FY 2026 Budget (July 2024): Budgeting for PQC transition

Quantum-Readiness: Migration to Post-Quantum Cryptography Factsheet (August 2023): Quantum readiness roadmap guidance

National Cybersecurity Strategy & Implementation Plan (March 2023): Post quantum strategic initiatives

Quantum Computing Cybersecurity Preparedness Act (December 2022): Mandated PQC planning

White House OMB Memo M-23-02 (November 2022): Crypto inventory & migration lead requirement

National Security Memo 10 (May 2022) Mitigating risks to quantum vulnerable cryptographic systems

Commercial National Security Algorithms Suite 2.0 (September 2022) PQC requirements for National Security Systems

THALES

Department of War Post Quantum Cryptographic Strategy (April 2026) The Department of War's (DoW) PQC Strategy defines a comprehensive framework for ensuring resilient, mission-ready cryptographic capabilities in the face of emerging quantum threats. It highlights quantum computing as an existential risk to national security systems, detailing how adversaries could exploit future quantum capabilities to decrypt sensitive data, compromise authentication, and disrupt command-and-control systems. To counter these risks, the strategy lays out five Lines of Effort focused on governance, enterprise-wide cryptographic inventory, development and analysis of quantum-resistant solutions, integration of secure commercial technologies, and deployment of quantum-resistant devices across DoW systems. The strategy mandates that all DoW systems must support PQC by 2030 and fully use PQC by 2031, ensuring that vulnerable algorithms are eliminated and replaced with quantum-resilient alternatives across all mission threads.

Committee on National Security Systems Policy 15 (March 2025 Revisions) The revised CNSS Policy 15 mandates a coordinated transition of national security systems from legacy public-key algorithms to NIST-approved post-quantum cryptography. It requires agencies to inventory cryptographic dependencies, prioritize systems that protect long-lived or high-value information, and adopt crypto-agile architectures that support PQC and hybrid implementations throughout the migration period. The policy aligns with CNSA 2.0 and NSM-10 timelines, directing modernization of hardware roots of trust, PKI, firmware signing, and key management to ensure quantum-resilient confidentiality and integrity across all mission systems.

Together, these directives establish a unified federal vision for achieving quantum readiness—pairing urgent security driven PQC requirements with long-term investments in modernization, innovation, and technology leadership. By laying out clear responsibilities, milestones, and technical expectations, the Federal Government has created an integrated framework that equips agencies to begin migrating today while preparing for tomorrow's quantum enabled capabilities. This coordinated approach ensures that the nation mitigates emerging cryptographic risks.

The Best Defense is Crypto Agility

As organizations prepare for the post-quantum era, crypto agility is becoming indispensable. Crypto-agile systems can adopt PQC algorithms quickly, minimize operational disruption, and remain resilient as standards evolve. Many long-standing cryptographic programs have already embraced these principles, giving them the architectural flexibility to absorb PQC's larger keys and increased computational demands with minimal friction.

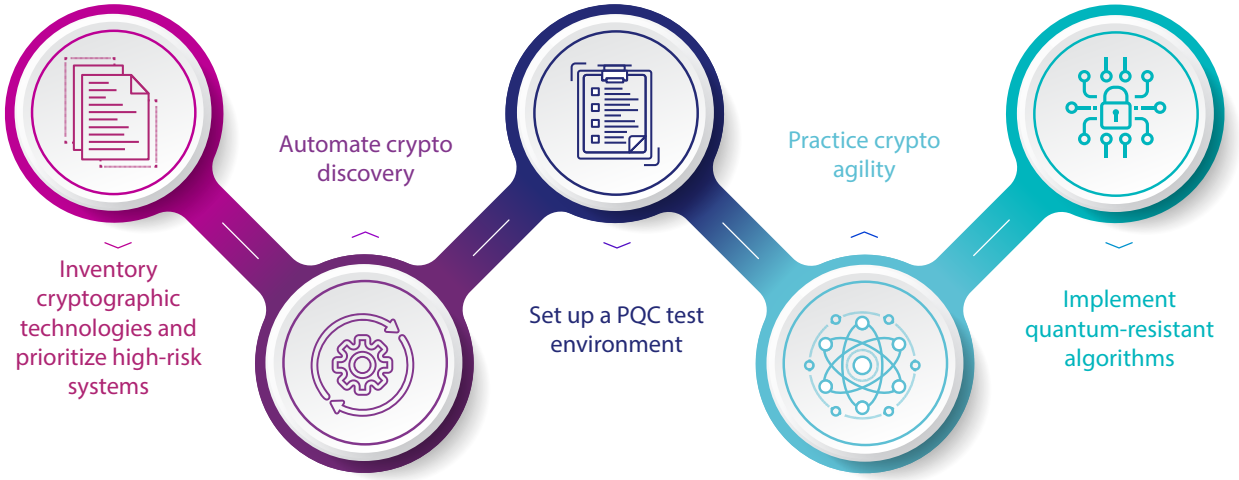
NIST's Cybersecurity White Paper **CSWP 39upd1** underscores this imperative, outlining the tradeoffs, operational complexities, and interoperability requirements involved in achieving true cryptographic agility. For federal agencies, the takeaway is clear: every modernization or procurement effort must require demonstrable crypto-agility, ensuring that systems purchased today can meet tomorrow's PQC mandates rather than becoming future technical debt. In short, crypto agility is no longer a theoretical best practice—it is a concrete acquisition requirement that protects mission longevity in the quantum era.



THALES

The Thales Five Step PQC Transition Strategy

Developing a successful PQC transition strategy requires a deliberate, phased approach. Agencies must build internal understanding of the quantum threat, establish a complete picture of their cryptographic landscape, and create the automation, testing, and agility needed to adopt PQC at scale. Thales has established a structured set of steps—from awareness and inventory to testing, agility, and implementation—organizations can follow to ensure a smooth, secure, and future-ready transition to quantum-resistant cryptography.



1. Inventory cryptographic technologies and prioritize high-risk systems.

Federal guidance makes clear that effective post-quantum migration begins with a complete and continuously updated inventory of all cryptographic technologies in use, since agencies cannot mitigate quantum risk without first understanding where vulnerable algorithms are deployed. OMB requires agencies to identify every instance of cryptography—especially those reliant on quantum-vulnerable public-key algorithms—and to maintain automated, continuously refreshed inventories that surface exposures across systems, including High Value Assets and high-impact environments. Similarly, the Department of War mandates a comprehensive accounting of all cryptographic components across assurance levels, reinforcing that planners must understand how legacy cryptography underpins mission-critical systems and where vulnerabilities present the greatest operational danger. Both authorities emphasize that inventory is inseparable from risk prioritization: agencies must assess which systems are most susceptible to cryptographically relevant quantum computer (CRQC) attacks and sequence PQC migration accordingly to ensure that high-risk, mission-critical, or sensitive systems receive immediate attention.

2. Automate crypto discovery.

Cryptographic technologies evolve constantly as systems change, software updates are deployed, and new services come online. Because of this dynamic environment, maintaining an accurate understanding of deployed cryptography cannot be a one-time effort—it must be a continuous, automated process. Both OMB and the Department of War emphasize that manual discovery is insufficient for keeping pace with modern IT environments and that agencies should leverage automated tools capable of identifying cryptographic functions, protocols, libraries, and embedded components across diverse systems. Automating crypto discovery ensures ongoing visibility into where quantum-vulnerable algorithms are used, increases accuracy compared to manual inventories, and rapidly detects changes as systems evolve. A wide range of commercial automated discovery and inventory solutions can help agencies sustain this continuous visibility and support the transition to post-quantum cryptography.

3. Set up a PQC test environment.

Agencies should establish a dedicated Post-Quantum Cryptography (PQC) test environment to evaluate how NIST-standardized algorithms perform within their operational ecosystems. OMB emphasizes that PQC migration must be integrated into system modernization efforts, requiring agencies to understand how new algorithms affect system performance, interoperability, and operational workflows before production deployment.

THALES

The Department of War likewise stresses the need to assess PQC solutions rigorously, ensuring they do not introduce new security risks, degrade mission capability, or conflict with existing architectures. Because PQC introduces larger key sizes, different computational properties, and new protocol behaviors, controlled testing is essential to identify bottlenecks, validate interoperability with existing systems and vendors, and ensure cryptographic agility. Agencies should use test environments to pilot early migrations, refine system integration plans, and validate that critical infrastructure can support PQC securely and efficiently

4. Practice crypto agility.

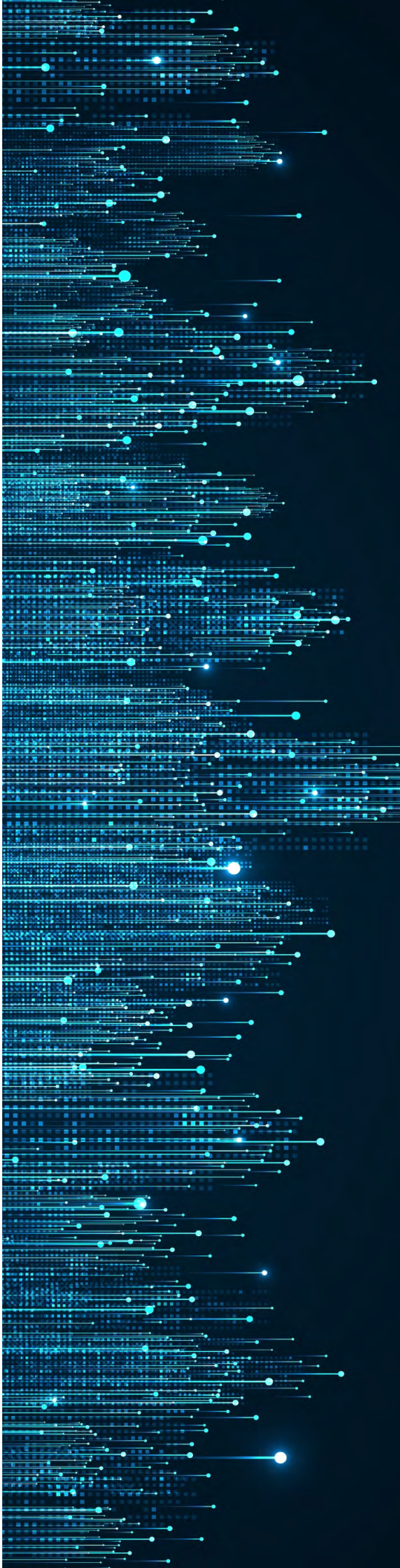
Prioritize crypto-agile solutions that can adopt PQC algorithms quickly, minimize disruption, and stay resilient as standards evolve. Modernize architectures so they can handle larger keys and heavier computation, and ensure every new technology purchase is both quantum-safe and crypto-agile.

Agencies should design and procure systems with built-in cryptographic agility, ensuring they can quickly adopt new algorithms as standards evolve and threats emerge. Crypto-agile architectures avoid hard-coded algorithms and allow cryptographic choices to be updated through configuration rather than system redesign. This adaptability is essential for transitioning to PQC and responding to future vulnerabilities. To support long-term resilience, agencies should ensure that every new technology purchase is both quantum-safe and crypto-agile, capable of integrating PQC algorithms today and evolving to meet tomorrow's requirements.

5. Implement quantum-resistant algorithms.

To meet federal PQC transition deadlines, organizations must ensure their systems begin adopting standardized quantum-resistant algorithms and maintain a clear, executable path for full migration. Implementing PQC is not optional—federal directives set firm dates by which systems must support and ultimately use quantum-safe cryptography, requiring organizations to modernize in advance of those milestones. Systems should be engineered or upgraded to integrate PQC algorithms now, or designed to be crypto-agile so they can transition smoothly as standards and requirements evolve. Ensuring that all new and existing technologies can adopt quantum-resistant algorithms enables agencies to stay ahead of mandated transition timelines and maintain secure, resilient operations as quantum-enabled threats emerge.

These five steps create a structured, federally aligned path for agencies to accelerate their PQC transition with confidence. By strengthening cryptographic visibility, enabling automated discovery, validating PQC performance early, adopting agile architectures, and implementing quantum-resistant algorithms on mandated timelines, agencies can minimize disruption while meeting government-directed requirements.



THALES

Strategic Alignment with Federal PQC Migration Frameworks

The table below highlights how Thales' modernization strategy directly maps to federal post-quantum migration phases and the Department of War's Lines of Effort (LOE). This alignment demonstrates clear strategic and operational parity with mandated PQC transition frameworks, ensuring Thales' solutions support mission readiness, compliance, and long-term cryptographic resilience.

Thales Step	OMB PQC Migration Phase(s)	DoW PQC LOE(s)	Key Deliverables
1. Inventory cryptographic technologies and prioritize high-risk systems	Phase 1 – Strategy, Planning & Discovery; informs prioritization in Phases 3–5	LOE 2 – Baseline Inventory & Plan; supports LOE 1 – Governance	• Enterprise cryptographic inventory (apps, devices, protocols, keys) • Risk-ranked system list (HVAs, high-impact systems) • Initial PQC migration prioritization matrix
2. Automate crypto discovery	Phase 1 with continuous use across Phases 2–5	LOE 2 – Baseline Inventory & Plan	• Automated crypto discovery tooling deployed • Continuous Cryptographic Bill of Materials (CBOM) • Dashboards for real-time crypto posture & policy compliance
3. Set up a PQC test environment	Phase 2 – Pilots & Early Migration, informing Phases 3–4	LOE 3 – Develop & Analyze; LOE 4 – Integrate Commercial Solutions	• PQC testbed environment • Performance + interoperability test results • Migration playbooks and validated integration patterns
4. Practice crypto agility	Begins in Phase 1–2, required across Phases 3–5	LOE 1 – Governance; LOE 4 – Integrate Commercial Solutions	• Crypto-agile architecture guidelines • Configuration-based algorithm selection mechanisms • Procurement requirements mandating quantum-safe + crypto-agile products
5. Implement quantum-resistant algorithms	Phase 3 – PQC for key establishment by 2030 Phase 4 – PQC for signatures by 2031 Phase 5 – Full migration by 2035	LOE 5 – Deploy Quantum-Resistant Devices; supports LOE 4	• PQC-enabled systems deployed • Decommissioning of quantum-vulnerable algorithms • Compliance with 2030 & 2031 federal deadlines; readiness tracking

PQC Execution Strategy

Thales TCT's PQC strategy is built on a multi-layered approach that ensures resilience, interoperability, and long-term adaptability across mission-critical environments.

Proactive Research and Development

Thales TCT maintains strong research partnerships with U.S. Government agencies to accelerate secure post-quantum adoption. Under a Cooperative Research and Development Agreement (CRADA) with the National Security Agency (NSA), Thales TCT is evaluating NIST-selected PQC algorithms operating within hardware security modules (HSMs). Insights from this work support Thales' accelerated deployment of PQC algorithms and help Government stakeholders understand how PQC-enabled HSMs mitigate quantum-era risks.

In parallel, Thales TCT serves as a founding participant in the NIST NCCoE Migration to PQC project and as a premier member of the Post-Quantum Cryptography Alliance, helping validate interoperability, assess performance impacts, and shape a cohesive, standards-aligned PQC ecosystem.

PQC Algorithm Adoption and Federal Compliance

Thales TCT has led the early integration of pre-standardized and now NIST-approved PQC algorithms across its HSMs, network encryptors, and key management systems. With federal mandates requiring quantum-capable National Security Systems (NSS) procurements beginning in 2027, the phase-out of non-compliant NSS by 2030, and civilian agency transitions to PQC spanning 2030–2035, Thales TCT delivers PQC-ready products well ahead of these deadlines—giving agencies the time and confidence needed to integrate and deploy quantum-resistant solutions effectively.

Crypto-Agile Architecture

All Thales TCT systems are engineered to transition seamlessly from classical to quantum-safe algorithms through configuration-based updates, minimizing operational disruption and ensuring long-term adaptability as standards evolve. This crypto-agility enables agencies to keep pace with emerging PQC requirements while maintaining mission continuity.

Customer Enablement

Thales TCT provides customers with guidance, tools, and training to evaluate existing cryptographic assets, plan their PQC adoption journey, and align migration strategies with Zero Trust principles and federal policy directives. This support ensures that agencies can execute their PQC transition with clarity and confidence.

PQC Capabilities Across the Thales TCT Portfolio

With the strategic foundation established, this section provides a detailed examination of how Thales TCT's PQC execution strategy is realized across our product portfolio. It outlines the current PQC readiness of each solution, the quantum-safe and crypto-agile capabilities already available, and the roadmap for integrating NIST-approved post-quantum algorithms. By presenting these technical details, we enable agencies to understand exactly how Thales TCT products can support their migration timelines, strengthen mission-critical systems, and meet evolving federal PQC requirements.

Protect Encryption Keys with T-Series Luna Hardware Security Modules

Hardware Security Modules (HSMs) are dedicated crypto processors that safeguard the entire cryptographic key lifecycle. They act as trust anchors, securely generating, storing, and managing keys inside hardened, tamper-resistant hardware. As organizations adopt post-quantum cryptography, HSMs become even more critical: they generate PQC keys for use in quantum safe solutions and provide performance, secure key storage, and controlled execution environment needed to handle PQC's larger keys and more complex algorithms without exposing sensitive material.

Luna T-Series HSMs are the choice for government agencies when storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States. Thales TCT's Luna T-Series HSMs were the first PQC-enabled HSMs manufactured in the U.S. to receive FIPS 140-3 Level 3 validation. Luna T-Series HSMs support the government's transition to post-quantum cryptography mandated by CNSA 2.0 and EO 14412. With support for ML-DSA, ML-KEM, and LMS/HSS, they safeguard long-lived and mission-critical data against emerging quantum threats.

Thales TCT's Luna T-Series HSMs contain an embedded QRNG chip for high-quality entropy based on quantum noise. All keys and random numbers generated within the HSM are enhanced by the security of the quantum random numbers that are the foundation of the key generation process.

THALES

Secure Data in Transit with High Speed Encryptors (HSE)

Thales High Speed Encryptors (HSE) provide quantum-resistant protection for data in motion across enterprise, government, defense and critical infrastructure networks. Designed to drop into a wide range of network architectures, from simple point-to-point links to meshed, hub-and-spoke and SD-WAN topologies, HSE is available as both physical and virtual platforms and delivers line-rate encryption at Network Layers 2, 3 and 4. PQC and hybrid modes have been built into certified HSE platforms, so customers can introduce quantum-resistant protection without adding external components or redesigning their networks.

Building on a long track record in high-assurance WAN and data-center protection, HSE hardware uses crypto-agile, FPGA-based designs so quantum-resistant capabilities can be enabled and updated via in-field firmware and policy changes. With NIST PQC algorithms implemented, HSE supports the transition from today's classical environments to PQC-ready networks, enabling hybrid classical/PQC tunnels so organizations can add quantum-safe protection while maintaining interoperability with existing devices and services.

HSE appliances carry a broad set of third-party validations, including FIPS 140-3 Level 3 validation (Level 1 for virtual models), Common Criteria certification, and approvals for government, defense and critical-infrastructure use via NATO NIAPC and the DoDIN APL, providing proven drop-in protection for traffic across public and private networks. Transport Independent Mode (TIM) delivers out-of-band key material using NIST-specified key-derivation functions, separating key delivery from the data plane to help mitigate Harvest Now, Decrypt Later threats.

Encrypt Data and Secure and Manage Keys from the Core to the Cloud to the Edge with CipherTrust Data Security Platform

The CipherTrust Data Security Platform (DSP) provides a data-centric foundation for PQC adoption. CipherTrust DSP discovers, classifies and protects sensitive data across databases, files, applications, cloud services and SaaS environments, to reduce data security risk. The platform centralizes key management, policy enforcement, tokenization, encryption, and supports quantum-safe key establishment in TLS servers and application environments using ML-KEM-based key exchange, while continuing to rely on Luna HSMs as the quantum-ready hardware root of trust for key generation, storage and critical cryptographic operations. This gives organizations a crypto-agile control plane to inventory cryptography, rotate keys, and re-encrypt sensitive data as PQC and hybrid algorithms are adopted.

Protect Identities and Control Access with Thales TCT Identity and Access Management Solutions

Thales Identity and Access Management (IAM) solutions extend quantum-ready security principles to digital identities and access control, addressing both current identity-based threats and the long-term cryptographic risks introduced by quantum computing. In modern zero-trust architectures, IAM must ensure trust not only in users, but also in the cryptographic mechanisms that underpin authentication, federation and secure access.

Thales IAM solutions, including PQC-ready authentication tokens and smartcards, hybrid-cloud credentials and identity management systems, are designed to accommodate the evolution of quantum-safe FIDO, PKI and TLS profiles, ensuring that passwordless authentication can be progressively aligned with post-quantum cryptographic foundations. This approach enables organizations to adopt phishing-resistant authentication today, while preparing for future PQC-enabled authentication tokens, smartcards, and protocols.

THALES

Conclusion

The transition to Post-Quantum Cryptography is a long-term undertaking—one that will take years for agencies to complete across all systems and mission environments. With cryptographically relevant quantum computers potentially emerging as early as 2030, agencies face a finite window to migrate to NIST's PQC standards and ensure the continued protection of sensitive data. In many ways, industry is already ahead, having spent years preparing for this shift so that federal agencies have the solutions, tools, and expertise needed to begin their own transitions.

Moving to a quantum-safe cryptographic ecosystem is complex, but entirely achievable with a structured approach. The steps outlined in this paper can help agencies navigate that journey. By automating crypto discovery, establishing a PQC test environment, practicing crypto agility, and implementing standardized PQC algorithms—starting with the highest-risk systems—agencies can position themselves for a successful and timely migration. The key is to begin now, while there is still time to transition securely and avoid future operational or mission risk.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

©2026 Thales 10.27.26