POST-QUANTUM CRYPTOGRAPHY

PQC Transition

A Systems Engineering Imperative

Dr. Ron Ross
RONROSSECURE, LLC

Based on NIST SP 800-160, Volumes 1 & 2

THE REAL PROBLEM

PQC Is Not Just a Cryptography Problem

The Common Framing

- Find vulnerable algorithms
- Swap for quantum-resistant ones
- Verify everything works

Result: Compliance without trustworthiness

The Real Challenge

Cryptography operates within an ecosystem of complex, interconnected, decades-old systems not designed with trustworthiness as an engineering outcome.

Replacing algorithms without fixing the underlying architecture is implementing gold-standard cryptography on a house of cards.

⚠ *SolarWinds 2020: Cryptographic code-signing was in place — and was bypassed entirely. The surrounding system was not engineered to be trustworthy.*

NIST SP 800-160, VOL. 1

Security Is an Emergent System Property

"Security is not a feature added to a system. It is an emergent property of a well-engineered system, arising from the deliberate application of sound engineering principles throughout the system lifecycle."

Designed In
Security emerges from engineering — not bolted on after the fact

Lifecycle-Wide
From concept development through disposal, every phase matters

Like Safety
As fundamental as safety in an airplane or reliability in a bridge

Many legacy systems violate this principle by design — built in an era when security was a stovepipe compliance activity rather than an engineered property tied to mission objectives.

PQC transition, as currently envisioned, inherits this deficiency. Organizations are applying new algorithms to architectures never engineered to support them.

Architectural Foundations for PQC

01

Domain Separation

Separate security domains with enforced boundaries. During migration, PQC-migrated systems must be architecturally isolated from legacy traditional-algorithm domains. Key management domains must be strictly separated from general-purpose computing environments.

02

Least Privilege

Each system element has only the access and authorizations necessary for its function. In many legacy systems, cryptographic keys are broadly accessible with no architectural enforcement — especially dangerous with agentic AI processes carrying excessive permissions.

03

Mediated Access

All access to system elements is mediated by an authorized control mechanism. PQC migration is the opportunity to route all cryptographic operations through a trusted mediation layer that enforces policy, logs access, and enables auditing.

Defense Architecture for PQC

04

Distributed Privilege

Multiple entities must collaborate for high-consequence operations. Key generation, escrow, rotation, and revocation require distributed authorization. Architectures allowing a single admin to act unilaterally are structurally vulnerable, regardless of algorithm strength.

05

Defense in Depth

Multiple layers of protection ensure that failure of one measure does not cause catastrophic compromise. Cryptography must be one layer among many — not the sole line of defense. When cryptographic protections are circumvented, additional architectural safeguards must limit damage.

06

Least Functionality

Provide only functionality necessary to support the intended mission. PQC migration paradoxically expands attack surface — hybrid mode requires both traditional and quantum-resistant algorithms simultaneously. Actively eliminate deprecated protocol versions and unused cryptographic services as migration progresses.

Resilient System Behavior

07 Protective Defaults

Default configurations must represent the most secure options. During PQC migration, the critical risk is that systems default to traditional-algorithm fallback for compatibility — defeating the migration for every negotiated-down connection.

PQC algorithms must be the default. Fallback to traditional algorithms must be an explicit, logged exception actively tracked.

08 Protective Failure

Systems must fail into a secure, known state. Legacy systems often fail open — component failure degrades security rather than orderly denial.

PQC migration into systems that fail open inherits this vulnerability. Stronger algorithms in an architecture that fails insecurely do not provide the protection they appear to on paper.

"Algorithm strength and system trustworthiness are not the same thing."

TRUSTWORTHY SECURE SYSTEMS

Algorithm Compliance ≠ System Trustworthiness

An organization can fully migrate to ML-KEM, ML-DSA, and SLH-DSA — achieve 100% algorithm compliance, satisfy every audit requirement — and still operate systems that are not trustworthy.

Why?

The underlying architecture has not been engineered to the design principles that produce a trustworthy secure system. The cryptography is stronger — but the system is not.

AI-driven cyberattacks — autonomous zero-day exploitation, multi-stage attack chains — are precisely the class of threat that exploits architectural weaknesses PQC migration leaves unaddressed.

Mission Resilience: The Four-Goal Framework

ANTICIPATE

Model adversary behavior across the full attack surface. A PQC-centric strategy does not anticipate supply chain, firmware, or architectural attacks that bypass cryptographic protections entirely.

WITHSTAND

Continue essential mission functions under active attack. Cryptographic protection supports this goal only if surrounding architecture can sustain mission functions when specific components are compromised.

RECOVER

Absorb an attack and continue operating. Recovery depends on knowing precisely what was compromised — requiring accountability, traceability, and supply chain assurance built into the architecture.

ADAPT

Evolve defenses in response to observed threats. Systems engineered for adaptability — modular, clean crypto interfaces — can absorb algorithm changes with manageable effort. Crypto-agility must be engineered deliberately.

PQC transition is a necessary condition for mission resilience — but it is not a sufficient one.

FROM THEORY TO ACTION

What This Means in Practice

Use PQC Transition as a Forcing Function

A once-in-a-generation opportunity to address decades of technical debt. Apply NIST SP 800-160 principles to enforce least privilege, reduce attack surface, and engineer defense in depth.

Inventory First — Then Go Deeper

Inventory reveals where cryptography lives. Systems engineering then asks: how does each mechanism interact with the surrounding system? What happens when it fails?

Architect for Cryptographic Agility

Clean separation between cryptographic mechanisms and applications, with well-defined interfaces and documented dependencies. Achieve agility now to handle future algorithm deprecations.

Rebuild PKI as a Systems Engineering Project

The federal PKI must be fundamentally re-architected — not patched. A ground-up rebuild of identity and trust across government with cascading dependencies requiring dedicated program resources.

Communicate in Mission Resilience Terms

Technical briefings on algorithm deprecation don't move budgets. Reframe: which critical functions are at risk, under which conditions, with what consequences. That argument reaches decision-makers.

CONCLUSION

The Systems Engineering Imperative

Necessary

The quantum threat is real. Harvest-now-decrypt-later attacks are already underway. PQC migration must happen.

Insufficient

Algorithm migration alone does not produce trustworthy systems. Security is an emergent property — not the result of compliance.

The Imperative

Use migration as the forcing function to build trustworthy, resilient systems with the engineering discipline SP 800-160 describes.

"The organizations that successfully navigate the quantum transition will not be the ones that finish algorithm migration fastest. They will be the ones that use migration as a forcing function to build the trustworthy, resilient systems that should have been built from the beginning."