



Post-Quantum Cryptography for Legacy and Migration-Constrained Systems in the Communications Sector

CSCC EMERGING TECHNOLOGIES COMMITTEE REPORT

Chairs	Jayati Dev, Alana Scott
Contributors	Jessica Almond, Ian Deakin, Vaibhav Garg, Todd Gibson
Contact	emerging-tech@CSCC-Full-Council.groups.io

EXECUTIVE SUMMARY

The transition to post-quantum cryptography (PQC) is essential for protecting communications networks and other critical infrastructure from future quantum-enabled attacks. Yet, migration remains challenging for legacy systems and other hardware, software, and protocols that cannot readily support cryptographic change.

This report examines the technical, operational, and governance constraints that complicate PQC deployment in the Communications Sector. It proposes a consistent, risk-based approach for assessing legacy assets and outlines practical migration and mitigation options that preserve operational continuity while reducing continued usage of quantum-vulnerable cryptography.

1. Introduction

Quantum computing could enable new approaches to select computational problems. At sufficient scale, it could also undermine quantum-vulnerable public-key cryptographic systems that protect confidential communications, verify digital signatures, authenticate devices, and establish trust across modern networks [2]. Continued reliance on these quantum-vulnerable algorithms presents a security risk that organizations must mitigate through timely migration to quantum-resistant cryptography or, where direct migration is not yet feasible, through appropriate interim protections.

The Communications Sector is working with industry and government to prepare for a post-quantum future. This effort requires a complex transition from quantum-vulnerable public-key cryptography to quantum-resistant algorithms and implementations across a number of systems. The transition will be particularly difficult in systems that cannot readily accommodate cryptographic change - including legacy and migration-constrained systems.

Migration Challenges Extend to Legacy Systems and Beyond

In a 2024 GDIT survey of 200 experts and decision-makers across U.S. defense, civilian, and intelligence agencies, 48% of respondents identified modernizing legacy systems as a significant challenge to PQC adoption. The survey describes federal respondents rather than the Communications Sector. Similar challenges are relevant to communications infrastructure, where long-lived systems are deeply embedded across public and private infrastructure and may be difficult to upgrade, maintain, or replace [1] [7].



Some current and recently deployed systems also face barriers due to fixed cryptographic implementations, hardware or software limitations, proprietary designs, certification constraints, vendor dependencies, or the absence of viable upgrade paths. Critical communications systems may need to remain operational for many years while these constraints are addressed.

Why Preparation Must Begin Now

The National Institute of Standards and Technology (NIST) notes that the future threat of quantum computers “may be years or decades away but could eventually break many of today’s widely used cryptographic systems.” Despite this uncertain timing, preparation is an immediate priority for the Communications Sector. Long implementation timelines, extended equipment lifecycles, and the possibility that adversaries are collecting encrypted data today for future decryption necessitate swift action [2].

2. Legacy and Migration-Constrained Systems

Legacy systems generally refer to older software, hardware, or protocols that remain in use due to deep integration, operational dependence, replacement cost, or the risk of service disruption. They are often resource-constrained, difficult to access, or no longer supported by the original supplier. However, age alone does not determine whether a system can migrate to PQC.

For this report, a migration-constrained system or component is any hardware, software, protocol, service, library, interface, or trust mechanism that cannot support the required cryptographic change within the necessary operational timeframe. This category can include both legacy assets and newer, current-generation equipment with fixed algorithms, insufficient processing or memory, proprietary software, certification restrictions, or no supported upgrade path.

Migration-Constrained Systems in the Communications Sector

The Communications Sector relies on a mixture of long-lived infrastructure and newer platforms, including servers, switches, routers, Cable Modem Termination Systems (CMTS), radio and core network equipment, processors, security appliances, operational technology, and management systems. Their upgrade timelines vary significantly, and even recently deployed products may be constrained by hardware design, firmware support, software dependencies, certification, or supplier roadmaps. The following examples illustrate systems that may be difficult to migrate, whether they are legacy or current-generation systems.

Older or fixed protocols: Hundreds of protocols are used across critical infrastructure. Some Industrial Control Systems (ICS), for example, use protocols such as traditional Modbus TCP/IP that were not designed with modern security controls. Other systems may continue to rely on older protocol versions or protocol designs with embedded classical algorithms. Even a current implementation can be migration-constrained where the protocol, message format, peer ecosystem, or interoperability requirements prevent the introduction of PQC without broader architectural change.

Operating systems and platform software: Some fielded hardware cannot support newer operating systems or cryptographic providers. Unsupported platforms such as Windows XP or Solaris versions that are no longer supported are clear examples, but newer systems may face similar restrictions where the operating system, firmware, boot chain, driver model, or vendor support agreement does not permit the required cryptographic updates.



Monitoring and operational systems: Communications and operational technology environments often use proprietary, specialized, or difficult-to-replace monitoring software. Unsupported libraries and insecure implementations may increase risk, but a newer platform can also be constrained where its application stack, vendor tooling, or integration dependencies do not support updated cryptographic libraries or protocols.

Obsolete or fixed cryptographic libraries: Legacy codebases may depend on outdated libraries that are no longer maintained. PyCrypto is one example of a well-known library with vulnerabilities. Current products may also be constrained when cryptographic libraries are embedded, proprietary, tightly coupled to applications, or cannot be replaced without recertifying the wider system [3]. These existing software vulnerabilities are distinct from susceptibility to future quantum attacks.

3. Technical, Operational, and Governance Challenges

Cryptographic algorithms and dependencies are present throughout communications of hardware, software, protocols, identities, trust infrastructures, and operational processes. Updating them is not simply a matter of installing a new algorithm. The feasibility of migration depends on the capabilities of each asset and the wider system in which it operates—and each asset varies significantly in age, architecture, performance requirements, vendor support, operational constraints, and existing [cryptographic agility](#).

The resulting challenges include technical constraints and operational and governance constraints.

Technical Challenges

Physical Hardware Limits: Hardware can be resource-constrained, with limited processing capability, power, storage, or memory sizes. Depending on the algorithm and parameter set, PQC can introduce larger keys, signatures, or ciphertexts that can exceed existing message sizes or buffer allocations. Failures may not be observable until the system is under load. While legacy devices may be especially susceptible, the same issue can arise in new equipment designed before PQC requirements were understood, or in current-generation products optimized for fixed performance, latency, or power envelopes [4][5].

Immutable Trust Anchors and Key Material: Some devices store cryptographic material in one-time programmable memory ("burned into" the silicon) or other immutable storage. In secure-boot designs, this may be a public key or public-key hash rather than a private key. Consequently, a device may have adequate compute and memory resources to support PQC while still lacking a supported way to update its trust anchor, associated verification algorithm, or other fixed key material. The exact restriction depends on the device design [9].

Hardcoded Algorithms: Even where memory and processing capacity are sufficient, communications equipment such as hardware security modules, secure elements, accelerators, network appliances, and embedded platforms may support only a hardcoded or vendor-defined set of algorithms. For example, traditional RADIUS deployments also contain cryptographic dependencies that require coordinated changes across communicating systems. Experimental RFC 9765 defines a RADIUS/1.1 profile for TLS/DTLS that removes MD5-based packet authentication and attribute obfuscation; removing MD5 does not itself complete a PQC transition [10]. Changing such implementations may require new firmware, re-engineered hardware roots of trust, changes to certificate parsing and key storage, recertification, or complete hardware replacement. These restrictions can affect both older products and recently deployed systems.

Side-Channel Vulnerabilities: Emerging research identifies side-channel and implementation-security risks in some PQC implementations. These findings do not represent breaks of standardized PQC algorithms; rather,



they highlight how implementation flaws, insufficient countermeasures, or platform-specific weaknesses can introduce vulnerabilities [13]. Introducing new algorithms on hardware that lack appropriate countermeasures, secure implementation guidance, or sufficient test coverage may create vulnerabilities even where the algorithm itself is standardized [16]. Any assessment must therefore consider not only whether PQC can run, but whether it can be implemented securely and reliably on the target platform.

Specialist Expertise for Legacy Systems: Modifying older software packages, libraries, and tightly integrated systems without disrupting other functions may require scarce expertise and specialized development platforms. This knowledge may reside with a small number of employees, suppliers, or original developers, creating both technical and continuity risks.

Verification and Observability Difficulties: Even when PQC transition policies exist, verifying the cryptographic posture of remote, embedded, proprietary, or otherwise opaque systems can be difficult. Inspecting firmware, secure boot configurations, certificate stores, libraries, and hardware security functions may require specialized tools or supplier support. Outdated development environments are one cause, but the same visibility problem can arise in new closed platforms. Limited observability also makes performance benchmarking and migration testing harder, increasing the risk of integration errors.

Operational and Governance Challenges

Asset ownership, vendor dependencies, risk management, budgeting and procurement cycles, asset lifecycle, and operational requirements can influence how and when systems can be upgraded, replaced, or retired.

Physical Constraints: Migration-constrained systems may be located in remote areas, embedded in operational environments, or deployed at a scale that makes inspection and replacement expensive. Risk-based decisions driven by cost, accessibility, supplier support, and operational constraints may lead organizations to accept residual quantum risk in parts of their infrastructure. This can result in uneven adoption across networks and regions. Less-resourced operators may face particularly difficult choices where critical equipment remains serviceable but lacks an affordable migration path.

Low Tolerance for Downtime: Communications and other critical infrastructure sectors have a low tolerance for operational failure. New cryptographic implementations may require extensive testing, certification, interoperability validation, and compliance review before new algorithms are deployed.

No Clear Line of Responsibility: If and when a compromise occurs, it can be difficult to assign liability. For legacy systems that often exist for decades, the original manufacturer may no longer exist or may have ended support. For current systems, the supplier may remain active but have no credible PQC roadmap, or the product may depend on proprietary hardware and software that the operator cannot modify. Clear ownership is therefore needed for assessing cryptographic exposure, obtaining supplier commitments, funding upgrades or replacement, approving temporary mitigations, and accepting residual risk.

Reliance on Vendor Cooperation: Even when their original manufacturers are available, many legacy systems depend on single, proprietary hardware vendors, making PQC upgrades difficult without vendor cooperation. This creates a policy dependence on providers that may not align with the enterprise users' needs, a challenge for both legacy and modernized systems. Operators may, therefore, need to balance the risk of continued reliance on quantum-vulnerable public-key cryptography against the safety, availability, and service-continuity risks of an inadequately tested change.



4. Assessment and Migration Choices

PQC migration should be managed as an ongoing risk-management and lifecycle-management challenge. The appropriate treatment depends on each asset's architecture, performance, interoperability, supplier support, operational criticality, and remaining service life.

NIST's migration project emphasizes identifying quantum-vulnerable cryptography and developing prioritized migration roadmaps. The assessment and treatment categories below are this report's synthesis informed by that guidance, rather than a formally prescribed NIST taxonomy [8].

Initial Migration Feasibility Assessment

Effective PQC migration begins with understanding where cryptography is used, how it is implemented, and whether affected assets can support the required changes. The initial "cryptography inventory" [14] should cover relevant hardware, software, protocols, certificates, keys, and other assets to help with today's migration and any future updates.

The assessment should not begin by asking whether a system is legacy; it should ask whether the system can support the required cryptographic change within the necessary timeframe. Factors should include current cryptographic dependencies, upgrade mechanisms, supplier support, processing and memory limits, protocol and interoperability constraints, information sensitivity and retention period, operational criticality, external exposure, remaining service life, and the feasibility of replacement.

Migration and Risk Treatment Choices

Based on the assessment, organizations can select one or more of the following treatments. Different assets may require different approaches, and temporary risk acceptance should accompany a defined transition plan.

Migrate: Upgrade the asset directly where supported PQC-capable software, firmware, protocols, or hardware are available and can be deployed safely.

Protect and Contain: Apply segmentation, isolation, restricted connectivity, strengthened access controls, enhanced monitoring, reduced data exposure, and quantum-safe protection at the closest technically feasible boundary where direct migration is not yet possible.

Replace or Retire: Establish a funded and time-bound replacement or decommissioning plan where the asset cannot be upgraded or adequately protected.

Adapt: Introduce middleware, protocol mediation, cryptographic gateways, or architectural changes where the asset cannot implement PQC natively but can use PQC protection on specified communications paths through a gateway or other boundary mechanism.

Temporarily Accept and Govern Residual Risk: In scenarios where a critical service must continue, and no immediate migration or replacement option exists, plan ahead by documenting the risk owner and adding compensating controls. Risk acceptance should be a temporary, managed transition state, not a permanent outcome.

5. Implementation and Interim Protections

Isolate and Segment Where Direct Migration Is Not Possible: Network segmentation is a potential temporary measure for systems that cannot yet support quantum-safe cryptography. An inventory process to identify affected assets and isolate them from unnecessary access is an important first step. Segmentation should be accompanied by explicit access policies, monitoring, logging, and a defined migration or replacement plan [6]. Segmentation reduces access and exposure; it does not make the asset's cryptography quantum resistant.

Legacy or migration-constrained subnets: Subnets built around classical cryptographic stacks, fixed protocols, or non-upgradable hardware can create boundaries where quantum-resistant protection cannot be applied end to end. These environments may require bridging architectures, gateways, or other forms of protocol mediation between PQC-secured domains and constrained systems, increasing architectural complexity, and potentially expanding the attack surface.

Operating System, Firmware, and Platform Updates: PQC affects foundational assets including cryptographic libraries, IPsec and TLS stacks, certificate handling, secure boot, key storage, and kernel or platform services. Operators should assess whether supported updates can enable migration and whether the supplier will maintain them for the required service life. Where the update path is absent, the asset should be moved to an adaptation, containment, replacement, or governed risk-acceptance path.

Testing and Validation Programs: Migration should be supported by pilots and rigorous testing for performance, message size, latency, interoperability, backward compatibility, failure behavior, side-channel exposure, and operational recovery. Rollback and contingency arrangements are necessary, but fallback to classical cryptography should be controlled to avoid creating an indefinite or exploitable downgrade path.

Middleware and Boundary Protection: Maintaining constrained systems alongside modern platforms may be necessary during extended transition periods. Potential approaches include encryption gateways, intermediate proxies, and crypto-agile mesh architectures. These can terminate quantum-safe protection near the constrained asset and mediate communications with the classical domain. Such mechanisms must be designed carefully because they introduce trust concentration, translation complexity, and additional attack surfaces. Protection applies only to the paths and cryptographic functions covered by the architecture. A gateway does not automatically upgrade a legacy endpoint's secure boot, digital signatures, stored-data protection, or the remaining classical connection [5].

API Warnings and Library Hygiene: Research published in 2018 studied API-integrated security advice to help developers avoid cryptographic API misuse. Such warnings can support cryptographic hygiene, but the study does not demonstrate PQC migration or establish deployment cost savings. Their role in staged migration should be evaluated alongside actual library and protocol upgrades [11].

Closed-Source and Unsupported Systems: Closed-source products create challenges when a supplier ceases operations, ends support, or declines to provide an upgrade. Open-source software does not guarantee maintenance, but access to source code may create additional options for community or third-party support. A 2024 engineering experience report on adding PQC support to selected Estonian e-government assets illustrates the potential for targeted modernization where source access and specialist expertise are available. This is an example of asset-level engineering work, not evidence of a completed nationwide migration or a guarantee of open-source maintenance [4].



Managing Quantum-Vulnerable Cryptography During Transition: Some critical infrastructure may need to remain in service for years even though its native protocols or cryptographic mechanisms cannot be upgraded. In these cases, organizations should determine how to operate the asset with managed and reduced risk. Options may include minimizing the sensitive data it handles, shortening data-retention periods, strengthening key management and credential rotation, restricting connectivity and administrative access, increasing anomaly detection and logging, and applying PQC protection at surrounding gateways or network boundaries. These controls do not make the underlying quantum-vulnerable algorithm quantum-safe; they are compensating measures intended to reduce exposure until migration, replacement, or retirement is feasible. Shorter local retention periods and credential rotation do not retroactively protect ciphertext already collected by an adversary. Quantum-vulnerable public-key mechanisms must be distinguished from symmetric cryptography such as AES, which has different quantum-security considerations [12].

6. Conclusion

A consistent assessment of legacy and newer migration-constrained assets—followed by an explicit decision to migrate, adapt, protect and contain, replace, retire, or temporarily accept residual risk—provides a practical path forward. This approach supports operational continuity while ensuring that reliance on quantum-vulnerable public-key cryptography is visible, governed, periodically reassessed, and tied to a defined transition plan.

For the Communications Sector, the scale, interdependence, and long service life of many systems make PQC migration a particularly complex undertaking. Success will depend not only on the availability of quantum-safe technologies, but also on coordinated planning, standards development, supplier support, and risk-based decision-making across the broader communications ecosystem. As standards, products, and deployment guidance continue to mature, organizations that begin preparing now will be better positioned to manage both the PQC transition and future cryptographic changes.

Industry groups like the Communications Sector Coordinating Council (CSCC) help strengthen our PQC posture, providing an avenue for members to become informed [15]. By facilitating continued collaboration and information sharing in an environment that brings together multiple informed perspectives offering sector-specific insights, the CSCC supports the Communications Sector's collective ability to manage post-quantum risk in legacy and other migration-constrained systems.

References

- [1] Madison Alder. Cyber Officials Cite Legacy Systems as Post-Quantum Readiness Challenge. FedScoop, October 16, 2024. <https://fedscoop.com/cyber-officials-cite-legacy-systems-as-post-quantum-readiness-challenge/>
- [2] NIST. Post-Quantum Cryptography. Updated August 5, 2026. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- [3] IBM. Security Bulletin: Vulnerability in pycrypto-2.6.1.tar.gz affects IBM Integrated Analytics System (CVE-2013-7459, CVE-2018-6594). <https://www.ibm.com/support/pages/security-bulletin-vulnerability-pycrypto-261targz-affects-ibm-integrated-analytics-system-cve-2013-7459-cve-2018-6594>
- [4] Petr Muzikant, Jan Willemson, and Peeter Laud. Migrating Some Legacy e-Governance Applications to Post-Quantum Cryptography. January 2024. Paper accompanying the fifth NIST PQC Standardization Conference.



<https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/migrating-some-legacy-e-governance-apps.pdf>

[5] ENISA. Post-Quantum Cryptography: Integration Study. October 2022.

<https://www.enisa.europa.eu/sites/default/files/publications/Post%20Quantum%20Cryptography-%20Integration%20Publication.pdf>

[6] Chuck Herrin. Apps, Networks, and Legacy Systems in the Quantum Crosshairs: A CISO's POV. F5, August 6, 2025. <https://www.f5.com/company/blog/apps-networks-and-legacy-systems-in-the-quantum-crosshairs-a-cisos-pov>

[7] GDIT. GDIT Research Study Finds 50% of Federal IT Leaders are Accelerating Strategies to Transition to Post-Quantum Cryptography. October 16, 2024. <https://www.gdit.com/about-gdit/press-releases/gdit-research-study-finds-50-of-federal-it-leaders-are-accelerating/>

[8] NIST NCCoE. Migration to Post-Quantum Cryptography. <https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc>

[9] Trusted Firmware-M. HW crypto key integration in TF-M secure boot. https://trustedfirmware-m.readthedocs.io/en/latest/design_docs/booting/secure_boot_hw_key_integration.html

[10] Alan DeKok. RADIUS/1.1: Leveraging Application-Layer Protocol Negotiation (ALPN) to Remove MD5. RFC 9765, Experimental, April 2025. <https://www.rfc-editor.org/rfc/rfc9765.html>

[11] Peter Leo Gorski et al. Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse. SOUPS 2018. <https://www.usenix.org/conference/soups2018/presentation/gorski>

[12] NIST. Post-Quantum Cryptography Frequently Asked Questions. <https://csrc.nist.gov/projects/post-quantum-cryptography/faqs>

[13] Yanning Ji, et al. A side-channel attack on a hardware implementation of CRYSTALS-Kyber. 2023 IEEE European Test Symposium (ETS). IEEE, 2023. <https://eprint.iacr.org/2022/1452>

[14] NIST SP 1800-38B. Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery. <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf>

[15] CSCC Emerging Tech Committee Report on Post-Quantum Cryptography. <https://comms-scc.org/2023/07/31/the-engineer-who-cried-quantum/>

[16] Fikret Garipay. Fault injection on PQC implementations. Black Hat USA 2025. <https://i.blackhat.com/BH-USA-25/Presentations/USA-25-Garipay-Bypassing-PQC-Signature-Verification-V2.pdf>