Human Factors in Design, Engineering, and Computing, Vol. 238, 2026, 2451–2459
https://doi.org/10.54941/ahfe1008470

A Cryptoagility-Driven Architectural Model for Post-Quantum Cryptography Migration in Edge and Access Networks

Reijo M. Savola

University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

The migration to Post-Quantum Cryptography (PQC) represents a systemic transformation of cybersecurity architectures, requiring not only algorithm replacement but also continuous cryptographic lifecycle governance across heterogeneous infrastructures. While standardization of PQC algorithms is progressing, organizations face significant challenges in deploying quantum-safe security across heterogeneous edge and access infrastructures characterized by constrained resources, long device lifecycles, and multi-vendor ecosystems. This paper presents a cryptoagility-driven model for PQC migration that supports controlled adaptation of cryptographic mechanisms while preserving operational continuity across heterogeneous infrastructures. The proposed model integrates continuous cryptographic inventory, centralized crypto-policy governance, algorithm abstraction, modular cryptographic services, hybrid classical-PQC operation, communication security, interoperability support, lifecycle management, and long-term data protection. Cryptographic agility is incorporated as a transversal architectural capability spanning governance, lifecycle management, communication security, and trust management functions, enabling runtime adaptation to evolving standards, emerging vulnerabilities, and changing operational requirements. The model addresses both technical and organizational aspects of migration while supporting scalable deployment across distributed edge and access environments. By combining layered architectural principles with dynamic cryptographic governance and lifecycle management, the proposed model provides a practical blueprint for achieving sustainable quantum-safe transformation in complex infrastructures.

Keywords: Post-quantum cryptography, Edge computing, Access networks, Quantum-safety

INTRODUCTION

The emergence of quantum computing presents a fundamental challenge to contemporary cybersecurity. Public-key cryptographic algorithms that underpin digital communications, authentication systems, and trust infrastructures are expected to become vulnerable once sufficiently capable quantum computers become available (Alagic et al., 2022). As a consequence, organizations worldwide are preparing for a transition toward Post-Quantum Cryptography (PQC). The release of the first NIST PQC standards (ML-KEM, ML-DSA, and SLH-DSA) has shifted the challenge from algorithm selection toward practical migration, deployment, interoperability, and lifecycle management. NIST SP 1800-38 (Newhouse et al., 2023) emphasize PQC

Received September 24, 2026; Revised October 25, 2026; Accepted October 31, 2026; Available online December 1, 2026

© 2026 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

migration preparation, interoperability testing, cryptographic discovery, and operational deployment challenges rather than algorithm selection.

Although considerable research has focused on quantum-resistant algorithms, the principal challenge of PQC migration lies in transforming the operational, architectural, and governance mechanisms that support cryptographic services. Cryptography is deeply embedded throughout information systems, communication protocols, operational processes, hardware platforms, software dependencies, and trust management infrastructures. Consequently, successful migration requires coordinated transformation of entire socio-technical ecosystems rather than isolated algorithmic upgrades (Barker et al., 2021; Näther et al., 2024). Protocols, applications, software, hardware, firmware, and infrastructures should be covered in this, rather than individual algorithms (Barker et al., 2025).

The challenge is particularly pronounced in edge and access network environments, in which operational constraints significantly complicate large-scale cryptographic transformations. Such infrastructures consist of large populations of geographically distributed devices, gateways, sensors, communication platforms, and management systems that often remain operational for decades (Roy et al., 2022). Migration decisions must remain robust under evolving cryptographic standards, changing threat landscapes, future cryptanalytic advances, and emerging operational requirements and technology platforms.

Consequently, the primary architectural challenge is not merely selecting suitable PQC algorithms but establishing mechanisms that enable continuous adaptation to evolving cryptographic requirements, standards, and risk assessments. This capability is commonly described as cryptoagility (Barker et al., 2025).

This study argues that cryptoagility constitutes the central architectural principle for achieving scalable and sustainable PQC migration. Rather than treating PQC as a static deployment objective, the study conceptualizes quantum-safe transformation as a continuous process of cryptographic adaptation and governance. Based on this perspective, we propose a cryptoagility-driven architectural model that enables organizations to manage continuous cryptographic evolution while maintaining operational stability, interoperability, and long-term security.

EDGE AND ACCESS NETWORKS: OPERATIONAL REQUIREMENTS FOR PQC MIGRATION

Edge and access infrastructures form a critical component of modern digital ecosystems. These environments span industrial automation systems, telecommunications networks, smart cities, connected transportation, healthcare systems, energy infrastructures, and Internet of Things (IoT) deployments. Their highly distributed and heterogeneous nature introduces significant technical, operational, and governance challenges. Edge environments commonly comprise heterogeneous computing nodes exhibiting substantial variation in processing capability, memory resources, communication technologies, and operational lifetimes.

Many devices remain deployed for decades and may lack sufficient resources to support computationally intensive cryptographic algorithms. (Das et al., 2021) Furthermore, access networks often involve multiple vendors, making interoperability and coordinated migration inherently complex (Roy et al., 2022).

The emergence of quantum threats amplifies these challenges. Sensitive information transmitted today may remain valuable long into the future, exposing organizations to harvest-now-decrypt-later attacks. Adversaries can collect encrypted data and store it until quantum computers become capable of breaking the underlying cryptography (Newhouse et al., 2023).

Operational constraints further complicate migration efforts. Resource limitations, large-scale deployments, intermittent connectivity, strict latency requirements, and fragmented technology ecosystems require migration approaches that are both flexible and highly manageable. Consequently, edge and access infrastructures constitute demanding deployment environments that require scalable and adaptable migration strategies (Näther et al., 2024). PQC migration is further complicated by the need to coordinate multiple stakeholders, including network operators, equipment vendors, software providers, and security governance functions. Migration decisions therefore extend beyond technical implementation and require organization-wide visibility into cryptographic dependencies and migration readiness (PQCC, 2025).

CRYPTOAGILITY AS THE FOUNDATION OF PQC MIGRATION

Historically, cryptographic technologies have often been integrated deeply into software, hardware, and operational processes. This architectural coupling increases migration complexity whenever cryptographic primitives require replacement due to vulnerability discoveries, deprecation, or evolving security requirements. The emergence of PQC exposes fundamental limitations in static cryptographic architectures that were not designed to accommodate frequent cryptographic transitions (Mosca et al., 2022).

Cryptoagility addresses this challenge by decoupling cryptographic functionality from dependent systems through abstraction, modularity, and policy-driven reconfiguration mechanisms. From this perspective, cryptographic mechanisms become replaceable components governed through policies, orchestration systems, and lifecycle management processes.

In a PQC context, cryptoagility enables (Barker et al., 2025):

- Dynamic algorithm substitution.
- Hybrid classical-PQC deployments.
- Flexible key and certificate management.
- Rapid response to newly discovered vulnerabilities.
- Continuous adaptation to evolving standards.
- Long-term maintainability of deployed systems.

Consequently, PQC migration should be viewed as a continuous lifecycle-management capability rather than a finite technology deployment project.

PROPOSED ARCHITECTURAL MODEL

The proposed architectural model conceptualizes PQC migration as a long-term cyber-resilience and lifecycle-management challenge in which cryptographic capabilities continuously evolve under governance control. The model treats cryptography as a dynamically governed service ecosystem in which policies, trust relationships, and cryptographic mechanisms evolve throughout the system lifecycle.

The proposed architectural model is structured around four mutually reinforcing capability domains: (1) Cryptographic Awareness, (2) Cryptographic Governance, (3) Cryptographic Adaptation, and (4) Cryptographic Resilience, as illustrated in Figure 1. Together, these domains form a holistic framework for managing cryptographic evolution throughout the system lifecycle. Cryptographic Awareness provides visibility into cryptographic assets, dependencies, protocols, trust relationships, and exposure to quantum-related risks. Building on this foundation, Cryptographic Governance translates organizational objectives and risk assessments into policies, migration priorities, and decision-making processes. Cryptographic Adaptation delivers the technical capabilities required to implement change through algorithm abstraction, hybrid classical-PQC deployments, certificate and key management, interoperability mechanisms, and controlled migration processes. Cryptographic Resilience ensures security and operational continuity by validating deployed controls and protecting data, software, devices, communications, and trust infrastructures against both current and emerging cryptographic threats.

The domains are interconnected through cryptoagility, which acts as a transversal capability spanning the entire architecture. Rather than treating PQC adoption as a one-time technology upgrade, the model establishes a continuous transformation cycle in which Awareness identifies assets, dependencies, and risks; governance converts these findings into policies and migration decisions; Adaptation implements the required changes; and resilience validates their effectiveness and operational impact. The outcomes of monitoring, assurance, and validation activities are continuously fed back into the Awareness and Governance domains, enabling architecture to evolve in response to emerging vulnerabilities, changing standards, technological advances, and evolving organizational requirements.

This closed-loop approach aligns with contemporary PQC migration roadmaps, such as (PQCC, 2025), which organize migration activities into preparation, assessment, implementation, and continuous monitoring phases. Within this context, awareness establishes the asset and dependency baseline, governance guides prioritization and planning, adaptation enables deployment and integration of new cryptographic capabilities, and resilience provides ongoing validation, recovery, and long-term assurance. Collectively, these capabilities support a risk-informed process of continuous cryptographic transformation rather than a finite migration project, ensuring that organizations can sustain cryptographic security throughout future technological and threat-driven changes.

Cryptographic Awareness

Effective cryptographic agility requires comprehensive visibility into deployed cryptographic assets and dependencies. Organizations cannot effectively govern, prioritize, or migrate cryptographic assets that remain undiscovered. Therefore, continuous discovery and inventory capabilities provide persistent awareness of cryptographic assets, algorithms, certificates, trust anchors, communication channels, software dependencies, and hardware security functions.

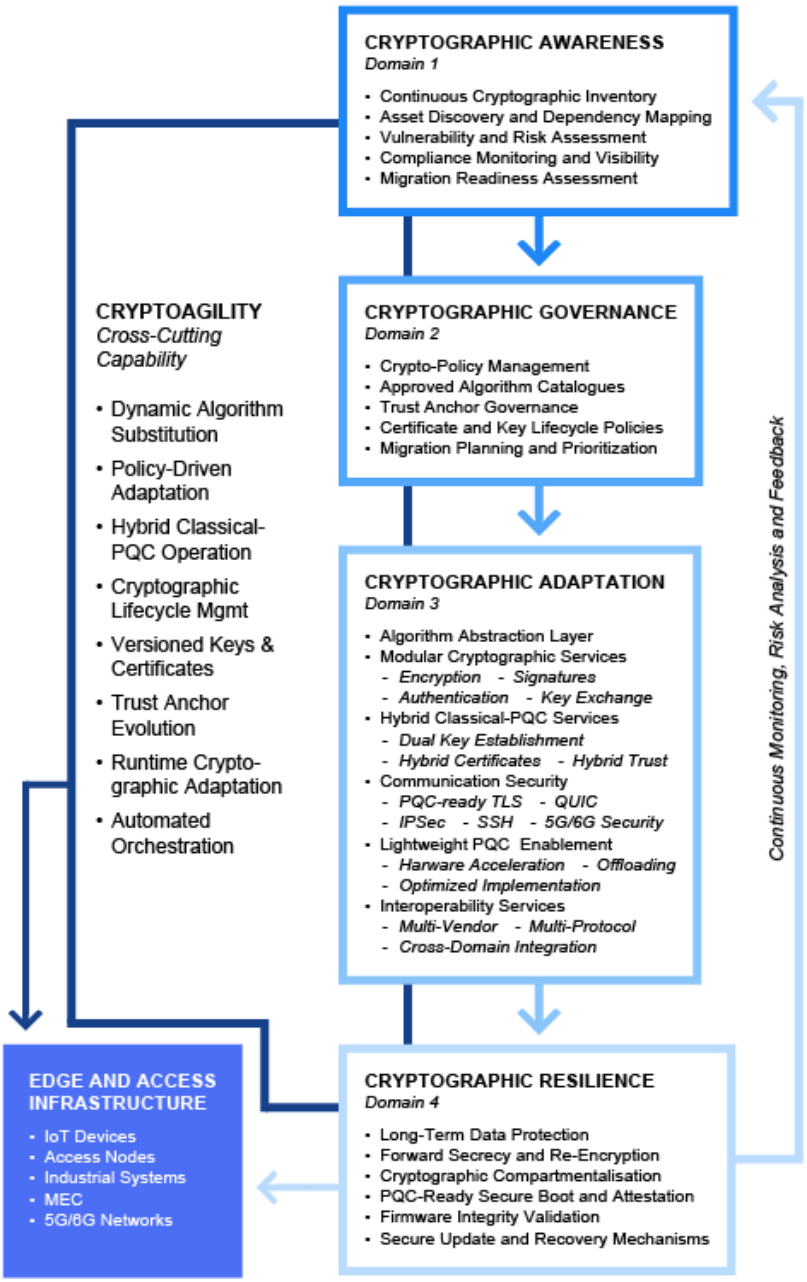


Figure 1: Proposed architectural model.

Such visibility provides the evidentiary basis for risk assessment, migration prioritization, compliance monitoring, and operational planning. Continuous cryptographic inventory management therefore becomes a foundational prerequisite for risk-informed cryptographic governance.

Recent migration programs increasingly rely on cryptographic discovery tooling, automated cryptographic inventory generation, and cryptographic asset classification to establish migration priorities and identify quantum-vulnerable dependencies across software, hardware, and network infrastructures (Newhouse et al., 2023).

Cryptographic Governance

Effective governance mechanisms are essential for ensuring policy consistency, regulatory compliance, and risk-based decision-making across large-scale distributed infrastructures. The Governance domain therefore serves as the strategic control layer connecting organizational security objectives with operational cryptographic transformation activities.

Policies define approved algorithms, migration strategies, trust requirements, certificate lifecycles, cryptographic strength levels, and hybrid deployment rules. Rather than statically configuring security mechanisms, systems continuously interpret and enforce cryptographic policies throughout their lifecycle. The governance domain therefore provides the linkage between strategic cryptographic objectives and operational deployment activities.

Migration studies further emphasize the importance of clearly defined stakeholder roles. Typical migration responsibilities include migration management, asset and risk management, security expertise, and technical implementation functions. Effective governance mechanisms should therefore support coordination across these organizational roles and responsibilities (Näther et al., 2024).

Cryptographic Adaptation

The Adaptation domain enables controlled modification of cryptographic mechanisms throughout operational lifecycles. The architecture enables adaptation through cryptographic abstraction, modular service design, and implementation independence. Applications and services consume cryptographic functions through stable interfaces while underlying implementations remain replaceable. Practical migration experiences demonstrate that adaptation mechanisms should support phased deployment strategies, interoperability between legacy and PQC-enabled components, and hybrid cryptographic solutions that combine classical and post-quantum algorithms during transition periods (Näther et al., 2024).

This approach enables:

- Introduction of new PQC algorithms.
- Retirement of vulnerable mechanisms.
- Hybrid classical-PQC operation.
- Dynamic trust-anchor updates.
- Runtime cryptographic reconfiguration.
- Automated lifecycle transitions.

As a result, cryptographic transitions can be executed incrementally and with reduced operational risk, enabling controlled evolution of production environments.

Cryptographic Resilience

Adaptation capabilities alone are insufficient unless cryptographic transitions can be executed without compromising operational continuity. The resilience domain ensures that cryptographic evolution can occur safely and continuously under changing circumstances.

This includes secure software updates, cryptographically agile certificate management, quantum-safe trust infrastructures, secure boot mechanisms, attestation frameworks, communication protocol evolution, and long-term protection of stored information.

Resilience further requires interoperability validation, continuous monitoring of deployed implementations, and readiness to respond to future cryptographic weaknesses or standardization updates without disrupting operational services.

Within the proposed framework, resilience extends beyond traditional cybersecurity objectives to include sustained resistance against cryptographic obsolescence and future technological disruption.

DISCUSSION

The proposed model extends existing PQC migration approaches by emphasizing architectural adaptability in addition to algorithmic modernization. This distinction is critical because quantum computing is unlikely to represent the final disruptive event affecting cryptographic security and trust infrastructures. Future advances in cryptanalysis, standardization, hardware architectures, and trust management frameworks may alter security requirements and deployment assumptions. Architectures tightly coupled to specific algorithms, trust models, or implementation technologies are expected to face significantly greater migration complexity as cryptographic ecosystems evolve. Architectures founded on cryptographic agility provide greater flexibility for accommodating future technological and standardization changes. The enduring value of PQC migration therefore lies not primarily in deploying new algorithms but in establishing organizational and technical capabilities for managing continuous cryptographic transformation.

Many current PQC migration efforts remain experimental, fragmented, and highly dependent on organization-specific practices. Reported challenges include insufficient PQC expertise, migration complexity, performance concerns, incomplete implementation support, legacy environments, and the absence of mature migration frameworks (Näther et al., 2024). The proposed architectural model addresses several of these challenges by emphasizing capabilities that support continuous visibility, governance, adaptation, and resilience across the cryptographic lifecycle.

Viewed from this perspective, cryptoagility becomes both the enabler of PQC migration and the enduring outcome of the migration process.

CONCLUSION

This study presented a cryptoagility-driven architectural model for systematic and sustainable migration toward post-quantum security in edge and access network environments. The model addresses the technical and operational challenges of cryptographic transformation by integrating awareness, governance, adaptation, and resilience capabilities within a unified architectural framework.

The proposed model reframes PQC migration as an ongoing process of cryptographic evolution. Instead of emphasizing static architectural layers, the model focuses on the capabilities required to sustain adaptation over decades of technological change: Cryptographic Awareness, Governance, Adaptation, and Resilience.

By embedding these capabilities throughout edge and access infrastructures, organizations can manage uncertainty associated with evolving PQC standards, emerging vulnerabilities, and future cryptographic transitions. The resulting architecture supports both near-term deployment of standardized PQC mechanisms and long-term management of cryptographic evolution across heterogeneous, multi-vendor, and resource-constrained infrastructures.

ACKNOWLEDGMENT

The work has been carried out in QU-ENABLER (Quantum-safety enabling infrastructures for edge intelligence in future networks) and SINTRA (Security of critical infrastructure by multi-modal dynamic sensing and AI) projects, co-funded by Business Finland and University of Jyväskylä.

REFERENCES

Alagic, G. et al. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. National Institute of Standards and Technology, NIST IR 8413.

Barker, W., Polk, W., Souppava, M. (2021). Getting ready for Post-Quantum Cryptography: Exploring challenges associated with adopting and using Post-Quantum Cryptographic algorithms. NIS Cybersecurity White Paper. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

Barker, E. et al. (2025). Considerations for Achieving Crypto Agility – Strategies and Practices. NIS Cybersecurity White Paper. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39-upd1.pdf

Das, A.K., Kumari, S., Li, X., and Wazid, M. (2021) Lightweight PostQuantum Cryptography for IoT Devices: Challenges and Solutions, IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10428–10445, 2021.

Mosca, M., Naehrig, M., Stebila, D. and Whyte, W. (2022) Quantum-Safe Cryptography: A Survey. ACM Computing Surveys (CSUR), vol. 55, no. 6, Article 120, pp. 1–38, 2022.

Newhouse et al. (2023) Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery. Volume B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools. NIST Special Publication 1800-38B. Available: https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

Näther, C., Herzinger, D., Gazdag, S., Steghöfer, J., Daum, S., Loebenberger, D. (2024). Migrating software systems towards Post-Quantum Cryptography – A systematic literature review. IEEE Access, 12, 132107-132126.

PQCC (2025). Post-Quantum Cryptography (PQC) migration roadmap. Post Quantum Cryptography Coalition. Available: https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf

Roy, S. S., Das, A. K., Chatterjee, S., Wazid, M. and Rodrigues, J. J. P. C. (2022) PostQuantum Cryptography for IoT and Edge Networks: Challenges and Directions, IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23430–23454, Dec. 2022.