Human Factors in Industrial and Systems Engineering, Vol. 219, 2026, 49–57
https://doi.org/10.54941/ahfe1007775

Quantum-Safety Enabling Cybersecurity Reference Infrastructure Model for Edge and Access Services

Reijo M. Savola

University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

The emergence of large-scale quantum computing threatens the long-term security of widely deployed public-key cryptography, creating an urgent need for quantum-safe migration across heterogeneous edge and access infrastructures. We present a scalable reference architecture that supports Post-Quantum Cryptography (PQC) adoption in resource-constrained, multi-vendor environments characteristic of edge and access services. The model integrates continuous cryptographic inventory, lightweight PQC for constrained devices, protocol-level modernization, interoperability, and crypto-agility, while addressing long-term data protection and device integrity across distributed systems. Our experimental setup demonstrates PQC-ready communication, secure cross-domain interactions, and AI-assisted monitoring under realistic edge-network conditions. The results provide a practical and extensible reference model for organizations seeking to reduce cryptographic exposure and transition toward quantum-safe security in complex, large-scale edge and access services.

Keywords: Cybersecurity, Post-quantum cryptography, Edge and access services, Critical infrastructures

INTRODUCTION

Quantum computing is widely regarded as a transformative technological paradigm with the potential to solve computational problems that are currently intractable for classical systems. Anticipated breakthroughs span diverse domains, including drug discovery, climate and weather modeling, large-scale optimization, and materials science. However, alongside these promising opportunities lies a profound cybersecurity challenge. Once sufficiently powerful quantum computers become available, they will be capable of efficiently solving the mathematical problems that underpin today's public-key cryptographic systems. As a result, many security mechanisms considered robust today may become obsolete in the near future.

The rapid progress in quantum technologies has intensified concerns regarding the long-term confidentiality and integrity of digital communications and critical infrastructures. A substantial portion of contemporary encryption—particularly asymmetric schemes used for key exchange, authentication, and digital signatures—could be rendered vulnerable to quantum-enabled attacks. This risk is especially acute for systems that require long-term data protection. Information encrypted today may be intercepted and stored by

Received February 19, 2026; Revised March 31, 2026; Accepted April 19, 2026; Available online July 20, 2026

adversaries, only to be decrypted retrospectively once quantum capabilities mature, a threat commonly referred to as *harvest now, decrypt later.*

Mitigating these risks requires more than the development of new Post-Quantum Cryptography (PQC) algorithms. While PQC standardization efforts are progressing, the broader challenge lies in enabling effective, scalable *migration* of existing infrastructures to quantum-safe architectures. Many organizations lack even a basic inventory of where cryptographic mechanisms are deployed within their systems, complicating the transition. Without systematic approaches, tools, and methodologies to support migration, the deployment of quantum-safe solutions may lag the pace of quantum technological advancement.

The urgency is underscored by the expected timeline: estimates suggest that viable quantum computers capable of breaking current asymmetric cryptography may emerge within the next decade. Given that many systems require data protection lifetimes of five to ten years or more, quantum-safe solutions must be adopted well before quantum computers reach full maturity. Failure to migrate in time could lead to silent compromise of critical infrastructures, with potentially severe societal and economic consequences.

Although practical large-scale quantum computers have not yet been realized, the threat they pose is already a present-day concern. All secret and private keys protected by current public-key algorithms, as well as the data encrypted under those keys, are at risk of future exposure. This includes stored information, archived communications, and any data transmitted over networks today. As modern critical systems—from energy grids to financial networks—rely extensively on public-key cryptography, the need for comprehensive quantum-safe migration strategies is both immediate and essential.

EDGE AND ACCESS SERVICES: ARCHITECTURAL BOUNDERIES, THREATS AND OPERATIONAL CONSTRAINTS

Edge computing is rapidly expanding across domains such as manufacturing, energy, smart cities, healthcare, logistics, and residential and mobile networks, creating complex multi-party ecosystems with increasingly large attack surfaces. Because quantum-vulnerable algorithms are deeply embedded in devices and infrastructure not designed for cryptographic upgrades, migrating to PQC will require coordinated replacement of hardware, libraries, protocols, and operational processes (PQCC, 2025). Quantum-safe infrastructures must therefore meet the unique demands of edge and access services, which operate under tight resource constraints, long device lifecycles, and highly distributed, heterogeneous environments.

These services span a diverse cloud–edge–device continuum with significant variation in hardware capabilities, protocol stacks, and vendor implementations. PQC migration must ensure interoperability, maintain performance across both powerful and constrained devices, and support long-lived deployments in remote or physically exposed locations. This architectural heterogeneity requires strategies that sustain distributed trust and seamless operation across the entire ecosystem.

Edge and access networks face both classical and quantum-enabled threats, including harvest-now-decrypt-later attacks, device tampering, protocol-downgrade exploits, supply-chain and update-channel compromises, and lateral movement across edge clusters (Näther et al., 2024). Addressing these risks demands PQC-ready identity, secure boot, authenticated update mechanisms, and robust session-establishment protocols.

Operational constraints further shape PQC adoption: limited device resources, high session density with strict latency requirements, intermittent connectivity, slow hardware-replacement cycles, large-scale deployments requiring automation, and sector-specific compliance obligations. These factors make lightweight PQC, crypto-agility, and automated lifecycle management essential for practical and secure migration (Egbuagha and Ikwunna, 2025).

Edge environments therefore demand quantum-resistant session establishment and lightweight cryptography (Turan et al., 2025), secure firmware and update channels (Alagic et al., 2022), and long-term data protection. At the same time, they face challenges such as limited computing resources, fragmented standards, interoperability issues, and the need for cryptographic agility as PQC algorithms evolve (ETSI, 2020).

TOWARDS POST-QUANTUM CRYPTOGRAPHY MIGRATION

Quantum computing poses a fundamental threat to modern cryptography. Once large-scale quantum computers emerge, all widely deployed asymmetric algorithms—RSA, elliptic-curve cryptography, and Diffie–Hellman—will be breakable, while symmetric algorithms, though more resilient, still require expanded key sizes and careful performance consideration in constrained environments. Despite this risk, most Information Technology (IT) and Operational Technology (OT) systems rely heavily on public-key cryptography, and few organizations maintain an inventory of where these algorithms are used. This creates a critical vulnerability: encrypted data harvested today may be decrypted in the future as quantum capabilities mature, exposing vast amounts of sensitive information (Bruze, 2021).

Although quantum-safe infrastructures and quantum key distribution technologies are advancing, their applicability to edge and access environments remains largely untested. Migration to PQC is far more complex than replacing algorithms; it requires coordinated updates across cryptographic libraries, validation tools, hardware accelerators, operating systems, application code, communication protocols, and administrative workflows. Security standards, operational procedures, and lifecycle-management documentation must also be revised or replaced (Barker et al., 2021). This represents a full-stack transformation rather than a simple cryptographic upgrade.

To date, most research has focused on algorithm design and performance benchmarking. However, leading security perspectives emphasize that quantum-safe transformation must be approached holistically integrating architectural considerations, operational constraints, deployment environments, and long-term use cases from the outset. Ensuring durable resilience requires embedding quantum-safe principles into the design, development, and governance of entire infrastructures, not merely substituting one algorithmic family for another.

PROPOSED MODEL

In the following, we introduce a scalable quantum-safe reference infrastructure model for edge and access services. The model covers common architecture, protocols, certificates, interoperation, processes, update issues, tools and requirements. The proposed model provides a scalable quantum-safe reference architecture for edge and access services, organizing PQC migration into layered capabilities suited to heterogeneous and resource-constrained environments. It spans continuous cryptographic inventory, lightweight and interoperable PQC, long-term data protection, and PQC-ready secure boot and update mechanisms. By structuring communication security, crypto-agility, and device integrity into a coherent framework, the model enables organizations to modernize protocol stacks, manage PQC performance impacts, and coordinate migration across large, multi-vendor deployments. The model reduces long-term cryptographic risk and enables a smooth, standards-aligned transition to quantum-safe security.

The layers of the model are grouped according to what the enable in the migration: foundational visibility, baseline PQC capability, cross-ecosystem operability, long-term resilience, and device and firmware trust.

Layer 1: Cryptographic Inventory as a Continuous Process – Foundational Visibility

A comprehensive and continuously updated cryptographic inventory is the single most important prerequisite for a successful transition to PQC. A clear understanding is needed of where cryptography is used, how it is implemented, and which systems depend on vulnerable algorithms (Alagic et al., 2022). Furthermore, PQC migration is not a one-time event. Solutions evolve, and the inventory should be maintained continuously, providing a factual baseline for prioritizing migration actions. Systems not able to support quantum-safe solutions must be identified as early as possible to be able to replace them in time (Chandre et al., 2024). Management and inventory can also be seen as the first maturity level of the infrastructure.

Layer 2: Lightweight PQC for Constrained Devices – Baseline PQC Capability

Some post-quantum algorithms introduce substantial computational overhead, which can overwhelm edge and access devices that operate with limited processing power and constrained battery capacity (Das et al., 2021). To keep these devices functional, responsive, and energy-efficient, quantum-safe infrastructures must provide lightweight PQC implementations tailored to constrained environments. This requires selecting efficient key-encapsulation and signature schemes, supporting hardware acceleration where available, and enabling policy-driven algorithm choices based on device capabilities.

Layer 3: Dedicated Layer for Communication Security – Protocol Foundations

A dedicated communication-security layer is essential for a practical and secure transition to post-quantum cryptography in edge and access networks.

These environments depend on diverse protocols—TLS, QUIC, DTLS, IPSec/IKEv2, SSH, WiFi EAPTLS (Das et al., 2023), and 5G/6G authentication (Bariah et al., 2022)—each progressing toward PQC readiness at different speeds. Because edge devices handle large volumes of secure sessions in multi-vendor ecosystems, quantum-safe infrastructures must ensure that session establishment, authentication, and key exchange remain robust, efficient, and interoperable throughout migration. This layer enables hybrid classical-PQC key exchange, PQC-resistant handshakes, downgrade-attack protection, and optimized session resumption, allowing devices with varying capabilities to negotiate PQC securely without breaking compatibility or degrading performance. By isolating communication security as its own layer, organizations gain a structured way to modernize protocol stacks, validate interoperability, and manage PQC's performance impact at scale.

Layer 4: Interoperability – Cross-Vendor and Cross-Protocol Operation

Quantum-safe infrastructures must remain interoperable across diverse protocols and multi-vendor environments, ensuring that PQC-enabled devices, services, and communication stacks can operate seamlessly despite differing standards, implementations, and hardware capabilities. This is because edge environments are inherently multi-vendor: access points, routers, IoT gateways, industrial sensors, and customer-premises equipment rarely come from a single supplier. (Roy et al., 2022) Without interoperability, these devices cannot authenticate, exchange keys, or establish secure channels with each other.

Layer 5: Crypto Agility – Future Proofing and Rapid Adaptation

As PQC standards continue to evolve—and as new cryptographic breakthroughs emerge—organizations must be able to rapidly update algorithms, keys, certificates, and trust anchors without disrupting critical services. The heterogeneity of edge and access devices makes rigid cryptographic implementations a major operational and security risk. (Mosca et al., 2022) Without agility, there is a risk deploying PQC algorithms that later prove inefficient, incompatible, or vulnerable, leaving large portions of the network stranded on obsolete cryptography. In short, cryptographic agility transforms PQC migration from a onetime upgrade into a sustainable, future-proof capability. For edge and access networks—where scale, diversity, and longevity amplify risk—agility is not optional. Key capabilities of the crypto agility include modular crypto libraries, versioned certificates and keys, and centralized crypto policy enforcement.

Layer 6: Long-Term Data Protection – Long-Term Resilience

Long-term data protection is a core requirement for achieving quantum-safe security in edge and access networks (Alagic et al., 2022). These environments continuously handle sensitive information—such as telemetry, credentials, logs, user data, and operational metrics—that must remain confidential

for many years. Because adversaries can already capture encrypted data today and decrypt it later once quantum computers mature, edge systems are especially vulnerable to harvest now, decrypt later attacks. To counter this risk, quantum-safe infrastructures must protect both data in motion and data at rest using algorithms resilient to future quantum capabilities. This includes adopting quantum-resistant symmetric encryption, using PQC key-encapsulation to secure keys, and ensuring end-to-end protection across storage, caches, and communication paths. With many edge devices operating unattended in untrusted environments, strong and durable cryptographic safeguards are essential.

Layer 7: PQC-Ready Secure Boot, Firmware Signing and Update Channels – Device and Firmware Trust

Ensuring firmware and software integrity is essential for quantum-safe security in edge and access networks, where devices often operate unattended, in untrusted environments, and for long lifecycles. A single compromised update can undermine the entire network, regardless of the strength of higher-layer cryptography. Quantum-safe infrastructures must therefore modernize secure boot and update mechanisms with PQC-resistant or hybrid signature schemes, protect long-lived trust anchors, and authenticate all update channels with quantum-safe integrity checks. These capabilities ensure that firmware, configuration, and software updates remain verifiably legitimate and tamper-free—even decades into the future (Regenscheid, 2018).

EXPERIMENTAL SETUP

An experimental setup was developed at the University of Jyväskylä to study post-quantum cryptography (PQC) migration in the context of edge and access services. The environment implements a secure, cross-domain architecture that enables controlled experimentation with PQC-ready communication, remote monitoring, analytics, and industrial control. It demonstrates how an OT domain—comprising industrial controllers, protocol servers, and physical production systems—interoperates safely with an IT and analytics domain providing remote access management, security operations, and AI-driven anomaly detection.

The domains are linked through a cryptographically protected communication channel designed to evaluate PQC-enabled and hybrid classical–PQC mechanisms. This channel ensures confidentiality, integrity, and authenticated access while allowing researchers to assess PQC performance, compatibility, and migration strategies under realistic edge-network conditions. Standardized industrial protocols expose OT-domain process data for real-time monitoring, predictive maintenance, and cyber-physical anomaly detection, while privileged-access controls regulate remote interactions with sensitive assets.

The setup reflects key architectural principles for PQC migration, including IT/OT segmentation, zero-trust remote access, protocol interoperability, AI-enhanced situational awareness, and cryptographic hardening. By integrating PQC-ready secure communication into a realistic

industrial environment, it provides a generalizable blueprint for deploying quantum-safe mechanisms in smart factories, critical infrastructure, distributed automation, and research–industry collaboration. The framework supports systematic experimentation with scalable PQC-ready edge and access architectures, enabling evaluation of migration paths, performance impacts, and operational feasibility while maintaining strong protection for industrial systems.

DISCUSSION

Successful PQC migration in edge and access environments requires more than technical upgrades; it depends equally on organizational readiness and socio-technical capability. Many organizations still lack a basic cryptographic inventory, underscoring the need for governance structures, operational competence, and workforce preparation to support hybrid deployments, crypto-agility, and long-term key management.

A critically missing dimension in most PQC migration efforts—and one addressed in this work—is the need for systematic risk modeling and assurance. Edge infrastructures face unique risks stemming from heterogeneous hardware, long device lifecycles, intermittent connectivity, and multi-vendor dependencies. PQC migration must therefore incorporate structured threat modeling for hybrid classical–PQC deployments, assurance criteria for PQC-enabled protocols and secure-boot chains, and verification mechanisms such as interoperability testing and continuous cryptographic posture monitoring. Residual-risk analysis is equally important for identifying legacy components and operational constraints that may limit PQC adoption.

Given the multi-vendor nature of edge ecosystems, coordinated migration timelines, interoperability testing, and trust-anchor updates across suppliers and operators are essential to avoid fragmentation. Sector-specific regulatory requirements must also be integrated into planning. By embedding socio-technical, organizational, and risk-assurance considerations into the migration process, the the result becomes not only technically feasible but also operationally sustainable and defensible across heterogeneous, large-scale deployments.

CONCLUSION

This work presents a scalable quantum-safe reference architecture tailored to the complex and resource-constrained nature of edge and access services. Achieving quantum-safe security in these environments requires coordinated changes across cryptographic libraries, hardware accelerators, operating systems, applications, communication protocols, and administrative workflows. The model emphasizes system-level feasibility, operational constraints, and long-term resilience rather than algorithmic substitution alone.

A central insight is the need for continuous cryptographic inventory, given the limited visibility many organizations have into where vulnerable public-key mechanisms are deployed. The model also reflects the constraints of edge systems—limited resources, long device lifecycles, intermittent

connectivity, and multi-vendor heterogeneity—which shape what forms of PQC are realistically deployable. Technical readiness alone is insufficient; effective migration requires strong cryptographic governance, coordinated cross-vendor planning, and workforce competence to manage hybrid deployments, crypto-agility, and trust-anchor updates. Equally important is the integration of risk modeling and assurance into PQC migration.

By integrating lightweight PQC, protocol modernization, interoperability, crypto-agility, and risk-assurance processes, the model provides a structured path for evolving heterogeneous ecosystems without disrupting critical services. Its focus on long-term data protection and PQC-ready secure boot and update mechanisms extends security beyond communication channels to device integrity and stored data, addressing persistent harvest-now-decrypt-later risks. Overall, the model demonstrates that quantum-safe transformation must be approached holistically—combining architectural, operational, organizational, and assurance-driven considerations—to ensure that edge and access infrastructures remain secure as quantum capabilities mature.

To support practical evaluation, an experimental setup was developed to test PQC-ready communication, hybrid classical–PQC mechanisms, and secure cross-domain interactions under realistic edge-network conditions. This environment provides empirical insight into performance impacts, interoperability challenges, and operational feasibility, strengthening the applicability of the proposed model.

Future work should validate and refine the proposed model through empirical studies in real deployments, with priorities including lightweight PQC benchmarking, multi-vendor interoperability testing, evaluation of crypto-agility mechanisms at scale, and development of automated tools for cryptographic inventory, policy-driven algorithm selection, and lifecycle management of PQC-enabled firmware and certificates.

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.

Bariah, M. B., Al-Fuqaha, A., Guizani, M. and Erbad, A. (2022) Post-Quantum Security for 6G Networks: A Survey, IEEE Network, vol. 36, no. 5, pp. 142–149, Sept.–Oct. 2022.

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

Bruze, E. (2021). Quantum as a disruptive technology in hybrid threats. European Commission, JRC Technical Report, 2021.

Chandre, P., Hingoliwala, H., Uttarkar, A., Shendkar, B. D., Lokare, D. and Sontakke, P. (2024) Post-Quantum Cryptography: Securing Critical Infrastructure Against Emerging Quantum Threats, 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 2024, pp. 1–7, doi: 10.1109/ICTBIG64922.2024.10911612.

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

Das, A. K., Kumari, S., Li, X., Wazid, M. and Obaidat, M. S. (2023) Post-Quantum Cryptography for Secure Communication: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 2543–2582, 2023.

Egbuagha, O. and Ikwunna, E. (2020). Post-Quantum Cryptography in practice: A literature review of protocol-level transitions and readiness. Cryptology ePrint Archive. Paper 2025/1668.

ETSI (2020). CYBER; Migration strategies and recommendations to quantum safe schemes. European Telecommunications Standards Institute (ETSI) Technical Committee Cyber Security, ETSI TR 103 619.

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.

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. arXiv: 2404.12854.

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

Regenscheid, A. (2018). Platform Firmware Resiliency Guidelines. NIST Special Publication 800-193.

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

Turan, M.S., McKay, K., Kang, J., Kelsey, J., Chang, D. (2025). Human Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions. National Institute of Standards and Technology, NIST SP800-232.