

Blind, Fragmented, and Out of Time: The Crypto-Agility Gap in PQC Migration

Markus Rautell

BUSINESS
FINLAND

Introduction

Motivation

- Quantum computing amplifies the long-recognized fragility of cryptographic longevity.
- Past transitions (e.g., MD5, SHA-1) were slow and incomplete, exposing systemic challenges in retiring weakened primitives.
- Security collapses rapidly when infrastructures cannot remove vulnerable mechanisms.
- Policy and standards bodies now enforce firm deprecation timelines, making routine cryptographic replacement an operational necessity.
- Real infrastructures may require 15+ years to transition due to deeply embedded cryptography, hardware refresh cycles, and supply-chain constraints.
- PQC migration highlights a structural weakness: global infrastructures lack the agility required for large-scale cryptographic updates.
- Without standardized abstraction and policy layers, organizations build bespoke and heterogeneous solutions that increase complexity and undermine interoperability.
- NIST stated in 2016 that agencies should be ready to replace current public-key algorithms within about 10 years and that maintaining crypto-agility was imperative [1]; however, few organizations acted on this guidance.

Core Concept

- **Capability:** Replace, update, or retire cryptographic mechanisms with minimal operational impact.
- **Visibility:** Accurate cryptographic inventories and CBoMs provide the asset awareness required for safe and sequenced transitions.
- **Modularity:** Algorithm-agnostic application design, clear abstraction layers, and policy-driven interfaces enable practical technical agility.
- **Governance:** Coordinated workflows and enterprise-level change management make transitions repeatable and sustainable.

Real-World Limitations and Research Gaps

The Invisible and the Undefined: Why Agility Fails Before It Begins

- No unified model of crypto-agility exists; definitions and architectural assumptions diverge across the literature, creating inconsistent design paradigms [2, 3].
- Ecosystem layers—including standards bodies, vendors, and enterprises—evolve at different speeds, producing structural misalignment that prevents coordinated PQC migration [4].
- Organizations frequently lack cryptographic inventories, dependency visibility, and governance structures, resulting in fragmented and often outdated knowledge of deployed cryptographic assets [5].
- Discovery practices remain immature: despite emerging standards such as CycloneDX [6, 7], tools vary in accuracy, lack automation, rarely differentiate initial discovery from continuous monitoring, and no widely adopted solutions support heterogeneous environments [3, 8].
- Visibility gaps across firmware, proprietary hardware, legacy middleware, and network equipment prevent reliable sequencing of system-wide cryptographic transitions [8, 9].
- No system-level mechanisms track migration issues across software stacks, hardware dependencies, protocols, and operational workflows, leaving organizations blind to end-to-end bottlenecks [10].
- Even when individual protocols become crypto-agile, the ecosystem lacks a unified architectural model to coordinate them, leaving migrations fragmented and undermining cross-layer PQC readiness [10].

Organizational Drag: The Migration Killer

- Cryptographic maintenance is routinely deprioritized under operational pressure; training burdens, distributed deployments, and logistical constraints lead to improvised and prolonged transitions that elevate security and operational risk [11].
- Enterprises lack practical orchestration mechanisms for transitioning non-agile, continuously operating systems, even though maturity models [12], risk frameworks [13], and high-level roadmaps [14, 15, 16] exist.
- Enterprise frameworks offer limited support for system-wide transitions, lacking structured processes for staged rollout, coordinated testing, rollback, and non-disruptive evolution across heterogeneous environments [5].
- Developers lack confidence in performing cryptographic updates, perceiving them as risky; this leads to delayed migrations, improvised fixes, and a persistent fear of breaking security [17].
- Most real-world cryptographic vulnerabilities stem from incorrect API use, insecure parameters, and misconfiguration; this indicates that developer knowledge gaps, not primitive weaknesses, remain a primary barrier to safe cryptographic evolution [18].
- PQC transition amplifies these human and organizational barriers: larger parameters, hybrid deployments, and legacy dependencies increase the complexity of non-agile environments [17, 19].

Project is funded by Business Finland, see www.pqc.fi for further information.

The Technical Debt Wall: Architecture and Tooling Failures

- Cryptographic mechanisms remain tightly coupled to application logic, and systems lack the abstraction layers, versioned metadata, and algorithm identifiers needed to support safe and controlled algorithm substitution [20, 3].
- Encrypted-data migration is obstructed by ciphertext formats that lack versioning or provenance markers, causing legacy encrypted data to accumulate as technical debt [3].
- Agile development and CI/CD pipelines fall short of cryptographic testing needs; they lack crypto-specific regression tests, downgrade-resistance checks, and structured rollout/rollback support [21, 20, 3].
- Testing support for PQC migration is inadequate: existing methods lack formal models of migration mechanisms, downgrade-attack analysis, and structured validation frameworks for assessing agility schemes [22].
- Developer tooling remains limited; automated discovery mechanisms, safe algorithm-substitution libraries, and end-to-end crypto-testing harnesses are largely absent [20].
- No comprehensive catalog of PQC migration challenges exists, hindering issue tracking, maturity assessment, and validation at scale [10].
- Actionable engineering methodologies and operational migration procedures remain missing, limiting the translation of research into deployable transition practices [3].

The Clock Is Ticking: External Forces Amplifying the Transition Gap

- Few available sources provide quantitative estimates, suggesting PQC migration may require 2–15+ years depending on enterprise size [23, 24], raising concern about alignment with current NIST and EU policy timelines [25, 16, 26].
- Aggressive early-2030s government deadlines leave little slack for legacy infrastructures that struggle with synchronized, large-scale updates [27].
- Migration costs estimates range from 250k\$ to over 1B\$, scaling with organizational size, system complexity, and required modernization efforts [28, 27].
- Vendors often treat cryptographic agility as a cost center without near-term benefit, creating economic and policy disincentives for timely migration [22].
- Limited international coordination leads countries to progress at uneven speeds, risking interoperability failures and inconsistent security guarantees across jurisdictions [27].
- Existing PQC guidance focuses on preparation and deployment, with limited support for detecting quantum-enabled compromise, responding to cryptographic failures, or recovering from hybrid-interoperability issues [29].
- Organizations lack a shared operational knowledge base. Early adopters report degradation, integration failures, and incompatibilities, but these lessons remain isolated, forcing others to rediscover the same pitfalls [29].
- Fallback, rollback, and recovery mechanisms for PQC failures remain largely unexplored [29].

The Missing Discipline of Cryptographic Transitions

- Research remains centered on primitives, proofs, and protocol behavior, while the engineering mechanics of real-world cryptographic transitions remain largely underdeveloped [30].
- Operational tasks essential for transitions (dependency management, multi-stakeholder coordination, and system evolution) receive far less attention than algorithm- and protocol-centric work [30].
- The field lacks lifecycle-oriented frameworks that treat agility as a system-wide engineering problem; few models explain how to plan, sequence, and execute transitions across heterogeneous infrastructures [30].
- Fragmentation across research domains (algorithm design, protocol evolution, systems engineering, governance) inhibits the development of integrated, end-to-end migration methodologies [4].
- Although agility is studied across technical, operational, organizational, and ecosystem layers, these insights have not yet matured into unified, transition-focused engineering approaches [4].

Closing the Transition Gap

- **We must establish shared models of agility and deploy automated, open-source cryptographic inventory and CBoM tooling so organizations can finally see what must be migrated.**
- **Organizations need coordinated governance, repeatable workflows, and trained teams to plan and execute cryptographic change at scale.**
- **Systems must adopt standardized crypto-agile abstraction and policy layers, supported by modular interfaces, versioned formats, and tooling for safe substitution and continuous transition.**
- **Migration planning must accelerate now, as long transition timelines and early-2030s deadlines demand immediate investment and international coordination.**
- **The field must develop a dedicated engineering discipline for cryptographic transitions, with lifecycle frameworks, metrics, and validated migration methodologies.**

References

- [1] Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray A Perlner, and Daniel Smith-Tone. *Report on post-quantum cryptography*, volume 12. US Department of Commerce, National Institute of Standards and Technology . . . , 2016.
- [2] Nouri Alnahawi, Nicolai Schmitt, Alexander Wiesmaier, Andreas Heinemann, and Tobias Graßmeyer. On the state of crypto agility. *Tagungsband zum*, 18:103–126, 2022. Accessed: 2026-01-12.
- [3] Guillaume Michel. Road to cryptographic agility. Diploma project (master's thesis), École Polytechnique Fédérale de Lausanne (EPFL), 2021.
- [4] Nouri Alnahawi, Alexander Wiesmaier, Tobias Grasmeyer, Julian Geißler, Alexander Zeier, Pia Bauspieß, and Andreas Heinemann. On the state of post-quantum cryptography migration. In *INFORMATIK 2021*, pages 907–941. Gesellschaft für Informatik, Bonn, 2021.
- [5] Dimitrios Sikeridis, David Ott, Sean Huntley, Shivali Sharma, Vasantha Kumar Dhanasekar, Megha Bansal, Akhilesh Kumar, Anwitha UN, Daniel Beveridge, and Sairam Veeraswamy. Elca: Introducing enterprise-level cryptographic agility for a post-quantum era. *Cryptology ePrint Archive*, 2023.
- [6] Ecma-424: Cyclonedx bill of materials specification, December 2025. Defines the CycloneDX v1.7 specification and includes the Cryptography Bill of Materials (CBOM) capability.
- [7] OWASP CycloneDX Project. *Authoritative Guide to CBOM: Implement Cryptography Bill of Materials for Post-Quantum Systems and Applications*. OWASP Foundation, 2024. Informative guidance; the normative standard is ECMA-424.
- [8] Brian LaMacchia. The long road ahead to transition to post-quantum cryptography. *Communications of the ACM*, 65(1):28–30, 2021.
- [9] Kyrylo Petrenko, Atefeh Mashatan, and Farid Shirazi. Assessing the quantum-resistant cryptographic agility of routing and switching it network infrastructure in a large-size financial organization. *Journal of Information Security and Applications*, 46:151–163, 2019.
- [10] Alexander Wiesmaier, Nouri Alnahawi, Tobias Grasmeyer, Julian Geißler, Alexander Zeier, Pia Bauspieß, and Andreas Heinemann. On pqc migration and crypto-agility. *arXiv preprint arXiv:2106.09599*, 2021.
- [11] Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, and Vaibhav Garg. Caraf: crypto agility risk assessment framework. *Journal of Cybersecurity*, 7(1):tyab013, 2021.
- [12] Julian Hohm, Andreas Heinemann, and Alexander Wiesmaier. Towards a maturity model for crypto-agility assessment. In *International Symposium on Foundations and Practice of Security*, pages 104–119. Springer, 2022.
- [13] Post-Quantum Cryptography (PQC) Working Group. Risk model technical paper, appendix a. Technical report, 2023. Accessed: 2026-01-05.
- [14] NSA CISA. Quantum-readiness: Migration to post-quantum cryptography. Technical report, CISA, Tech. Rep, 2023.
- [15] Post-Quantum Cryptography Coalition (PQCC). Post-quantum cryptography (pqc) migration roadmap. Technical report, MITRE Corporation, May 2025. Approved for public release. Distribution unlimited. 24-03931-7.
- [16] Commission recommendation on a coordinated implementation roadmap for the transition to post-quantum cryptography. Commission Recommendation C(2024) 2393 final, European Commission, Brussels, April 2024.
- [17] Alexander Krause, Harjot Kaur, Jan H Klemmer, Oliver Wiese, and Sascha Fahl. “that’s my perspective from 30 years of doing this”: An interview study on practices, experiences, and challenges of updating cryptographic code. In *In 34th USENIX Security Symposium*, 2025.
- [18] Stefan Krüger, Sarah Nadi, Michael Reif, Karim Ali, Mira Mezini, Eric Bodden, Florian Göpfert, Felix Günther, Christian Weinert, Daniel Demmler, et al. Cognicrypt: Supporting developers in using cryptography. In *2017 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 931–936. IEEE, 2017.
- [19] Lynette I Millett and Anne Frances Johnson. *Cryptographic Agility and Interoperability: Proceedings of a Workshop*. National Academies Press, 2017.
- [20] Lodovica Marchesi, Michele Marchesi, and Roberto Tonelli. A survey on cryptoagility and agile practices in the light of quantum resistance. *Information and Software Technology*, 178:107604, 2025.
- [21] Lodovica Marchesi, Michele Marchesi, and Roberto Tonelli. Reviewing crypto-agility and quantum resistance in the light of agile practices. In *International Conference on Agile Software Development*, pages 213–221. Springer, 2022.
- [22] David Ott, Christopher Peikert, et al. Identifying research challenges in post quantum cryptography migration and cryptographic agility. *arXiv preprint arXiv:1909.07353*, 2019.
- [23] Robert Campbell. Enterprise migration to post-quantum cryptography: Timeline analysis and strategic frameworks. *Computers*, 15(1), 2026.
- [24] TNO. Guidelines for migrating to post-quantum cryptography, 2024. Accessed: 24 April 2026.
- [25] Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson, and David Cooper. Transition to post-quantum cryptography standards. NIST Internal Report (IR) NIST IR 8547 ipd, National Institute of Standards and Technology, 2024.
- [26] A coordinated implementation roadmap for the transition to post-quantum cryptography. part 1, version 1.1. Technical report, NIS Cooperation Group Work Stream on Post-Quantum Cryptography, Brussels, June 2025. First deliverable following the European Commission Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.
- [27] Brian LaMacchia, Matt Campagna, and William Gropp. The post-quantum cryptography transition: Making progress, but still a long road ahead. *arXiv preprint arXiv:2503.04806*, 2025.
- [28] Volkan Erol. Quantum readiness in cryptography: A maturity-based framework for post-quantum transition. *Preprints*, October 2025.
- [29] Abdullah Aydeger, Engin Zeydan, Awaneesh Kumar Yadav, Kasun T Hemachandra, and Madhusanka Liyanage. Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *2024 15th International Conference on Network of the Future (NoF)*, pages 195–203. IEEE, 2024.
- [30] David Ott, Kenny Paterson, and Dennis Moreau. Where is the research on cryptographic transition and agility? *Communications of the ACM*, 66(4):29–32, 2023.