Beyond the Limits of PQC

The PQC Transition and Beyond: Gap Between Concept and Reality

Markus Rautell

BUSINESS FINLAND

Introduction

Motivation

- Quantum computing amplifies the long-recognized fragility of cryptographic longevity.
- Past transitions have been slow (e.g., DES, SHA-1), some of which have taken over a decade to complete, and PQC transition is anticipated to be more complex than any other before [1, 2].
- PQC migration is challenging because cryptography is deeply embedded in complex, large-scale infrastructures, turning migration into an enterprise-level problem [3].
- The inability to replace vulnerable cryptographic mechanisms in a timely manner increases systemic security risk.
- Policy and standards bodies increasingly define firm deprecation timelines, making routine cryptographic replacement an operational necessity.
- Despite early guidance on preparing for post-quantum migration [4], progress toward adopting crypto-agility and cryptographic inventory practices remains limited.

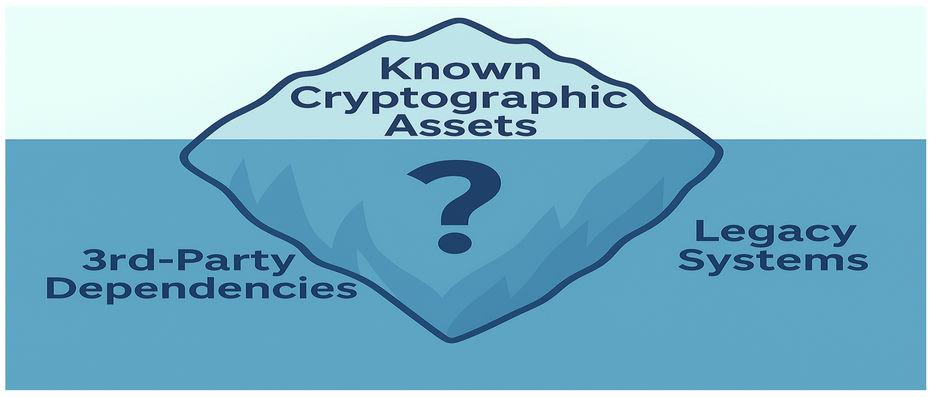
Core Concepts

- **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**: Crypto-agnostic application design with clear abstractions and policy interface enable practical agility.
- **Governance**: Coordinated workflows and enterprise-level change management make transitions repeatable and sustainable.

Real-World Limitations and Research Gaps

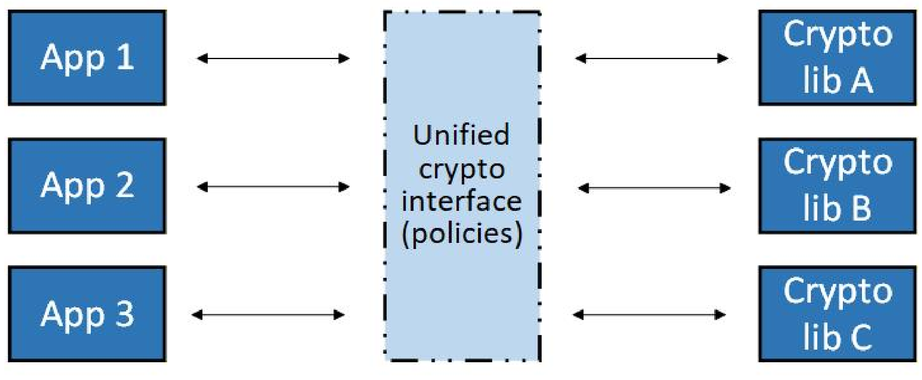
Limitations in Cryptographic Asset Visibility

- Visibility into cryptographic assets is widely identified as a key prerequisite for cryptographic transitions [5, 6, 7, 8]
- Multiple sources indicate that organizations often lack comprehensive visibility into their cryptographic assets [9, 10, 11, 8].
- Creating and maintaining comprehensive cryptographic inventories is widely reported to be challenging in practice, due to complex system dependencies, incomplete asset visibility, and organizational constraints [12, 13, 8].
- As CBOM standardization has only recently emerged [14, 15], available academic and practitioner evidence suggests that the associated tooling ecosystem remains immature and evolving [16, 17].



Fragmentation and Complexity in Crypto-Agility

- Many systems were not originally designed for cryptographic change: tightly coupled implementations and historically static design decisions make updates or algorithm replacements difficult without significant modifications [1, 18].
- Early and recent studies highlight the absence of a unified definition of crypto-agility, noting that a precise and concrete definition remains difficult to establish [19, 20].
- The identified need for universal cryptographic interface designs [1] suggests that widely adopted abstractions for achieving crypto-agility are still lacking, which can lead to heterogeneous implementations that reduce interoperability.
- Introducing crypto-agility increases system complexity, which may in turn expand the attack surface [1, 21].



External Constraints on Cryptographic Transitions

- Few available sources provide quantitative estimates, suggesting PQC migration may require 2–15+ years depending on enterprise size [22, 23, 24], raising concerns about alignment with current policy timelines (e.g., NIST, UK, EU) [2, 25, 26].
- As standardization efforts remain ongoing [27, 28], the limited time available for migration further emphasizes the need for agile adoption.
- A wide range of sources indicate that the PQC transition imposes a sustained economic burden, with cost and budget constraints consistently identified as significant barriers to adoption [29, 30, 31, 32, 33].
- Taken together with the widely held view that the PQC transition exceeds previous cryptographic transitions in scope and complexity [1, 2], the estimated timelines and economic constraints outlined above suggest that current policy timelines can reasonably be described as aggressive [29] and challenging to meet.
- Insufficient international coordination during the PQC transition may contribute to diverging implementation approaches and standardization practices, potentially leading to ecosystem fragmentation and complicating interoperability across PQC-compliant systems and protocols [29, 33].

Organizational Drag in Cryptographic Migration

- Prior work [34] indicates that cryptographic maintenance may be deprioritized under operational pressure, leading to ad hoc and prolonged transitions, a finding supported by interview evidence suggesting that such updates are often delayed or skipped in practice due to competing priorities and unclear benefits [35].
- Recent work [3] identifies limitations in prior crypto-agility approaches and proposes an enterprise-level architecture, but concrete methodologies for evolving existing systems toward such architectures remain lacking.
- From an enterprise-level perspective [3], control over cryptographic configuration is often limited at the organizational level, further complicating coordinated cryptographic change.
- An interview study [35] indicates that structured processes for cryptographic updates are often lacking in practice, complicating the systematic management of such transitions.
- This indicated lack of structured support is reflected at the developer level, where developers often report limited expertise, guidance, and confidence in performing cryptographic updates, leading to uncertainty and hesitation that can contribute to delayed, ad hoc, or skipped update practices [35].

Lack of Systematic Cryptographic Transition Engineering

- An early survey [36] is consistent with our observation that the literature predominantly focuses on PQC algorithms and protocol integration, while higher-level concerns such as migration and system-level transition strategies remain comparatively underexplored and are identified as open challenges.
- Prior work [20, 37] indicates that guidance for cryptographic migration remains largely abstract and incomplete, leaving much of the practical realization to practitioners.
- Building on both the literature [20, 37] and our observations, concrete engineering methodologies for achieving crypto-agility appear to be lacking.

Closing the Transition Gap

- **Develop and deploy automated, open-source cryptographic inventory and CBOM tooling to enable visibility into cryptographic assets.**
- **Establish shared models for crypto-agility along with standardized abstractions and policy interfaces to support modular, crypto-agnostic system architectures.**
- **Implement coordinated governance, repeatable workflows, and dedicated support to enable organizations to manage cryptographic change at scale.**
- **Accelerate migration planning to align with long transition timelines and early-2030s policy deadlines, requiring immediate investment and international coordination.**
- **Develop a dedicated engineering discipline for cryptographic transitions, including lifecycle frameworks, metrics, and validated methodologies for achieving crypto-agility.**

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

Contact: Markus Rautell, Research Scientist
Tel. +358 50 531 5094, markus.rautell@vtt.fi

References

[1] Elaine Barker, Lily Chen, David Cooper, Dustin Moody, Andrew Regenscheid, Murugiah Souppaya, Bill Newhouse, Russ Housley, Sean Turner, William Barker, and Karen Kent. Considerations for achieving crypto agility: Strategies and practices. NIST Cybersecurity White Paper NIST CSWP 39, National Institute of Standards and Technology, Gaithersburg, MD, 2025.

[2] 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.

[3] 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.

[4] 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.

[5] Microsoft Security Blog. Building your cryptographic inventory: A customer strategy for cryptographic posture management, April 2026. Accessed: 2026-05-14.

[6] Cryptographic inventory guide, December 2024. Accessed: 2026-05-18.

[7] Nicolai Schmitt, Johanna Henrich, Dominik Heinz, Nouri Alnahawi, and Alexander Wiesmaier. On criteria and tooling for cryptographic inventories. In *Sicherheit 2024*, pages 49–63. Gesellschaft für Informatik eV, 2024.

[8] Ponemon Institute LLC. 2026 global state of post-quantum and cryptographic security trends. Technical report, Entrust, January 2026. Sponsored by Entrust.

[9] NSA CISA. Quantum-readiness: Migration to post-quantum cryptography. Technical report, CISA, Tech. Rep, 2023.

[10] Marin Ivezic. Dos & don'ts of crypto inventories for quantum readiness, 2024. Accessed: 2026-05-14.

[11] Estevenson Solano. Cryptographic inventory: Key to visibility, digital trust and post-quantum readiness, nov 2025. Accessed: 2026-05-18.

[12] Mohib Ur Rehman. Why cryptographic discovery matters for post-quantum security, may 2026. Accessed: 2026-05-14.

[13] Marin Ivezic. How to perform a comprehensive quantum readiness cryptographic inventory, April 2024. Accessed: 2026-05-14.

[14] Ecma-424: Cyclonedx bill of materials specification, December 2025. Defines the CycloneDX v1.7 specification and includes the Cryptography Bill of Materials (CBOM) capability.

[15] 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.

[16] Roman Bögli, Jonas Spieler, and Timo Kehrer. BF-CBOM: Uncovering cryptographic assets through comparative CBOM analysis at scale. In *Proceedings of the 34th IEEE/ACM International Conference on Program Comprehension (ICPC 2026)*, pages 1–5, Rio de Janeiro, Brazil, 2026. ACM. Preprint - Accepted for publication.

[17] Unsung Limited. Cbom explained: Why you need a cryptographic bill of materials, January 2026. Accessed: 2026-05-19.

[18] National Institute of Standards and Technology. Migration to post-quantum cryptography: Preparation for considering the implementation and adoption of quantum safe cryptography. NIST Special Publication (NCCoE Practice Guide) SP 1800-38A, National Institute of Standards and Technology, 2023. Draft.

[19] 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.

[20] Christian Näther, Daniel Herzinger, Stefan-Lukas Gazdag, Jan-Philipp Steghöfer, Simon Daum, and Daniel Loebenberger. Migrating software systems toward post-quantum cryptography-a systematic literature review. *IEEE access*, 12:132107–132126, 2024.

[21] David Ott, Christopher Peikert, et al. Identifying research challenges in post quantum cryptography migration and cryptographic agility. *arXiv preprint arXiv:1909.07353*, 2019.

[22] Robert Campbell. Enterprise migration to post-quantum cryptography: Timeline analysis and strategic frameworks. *Computers*, 15(1), 2026.

[23] TNO. Guidelines for migrating to post-quantum cryptography, 2024. Accessed: 24 April 2026.

[24] Pqc migration planning, December 2024. Accessed: 2026-05-18.

[25] 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.

[26] National Cyber Security Centre (UK). Timelines for migration to post-quantum cryptography, 2023. Accessed: 24 April 2026.

[27] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Hung Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, and Noah Waller. Status report on the fourth round of the nist post-quantum cryptography standardization process. NIST Internal Report NIST IR 8545, National Institute of Standards and Technology, 2025.

[28] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, Quynh Dang, Thinh Hung Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, and Noah Waller. Status report on the second round of the additional digital signature schemes for the nist post-quantum cryptography standardization process. NIST Internal Report NIST IR 8610, National Institute of Standards and Technology, 2026.

[29] 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.

[30] Office of Management and Budget. Report on Post-Quantum Cryptography. Technical report, Executive Office of the President of the United States, July 2024.

[31] Department for Science, Innovation and Technology. Regulator and Industry Perspectives on the Current Plan for PQC Transition. Technical report, UK Government, November 2025.

[32] State of PQC Readiness: Are Businesses Prepared For Q-Day? Technical report, Trusted Computing Group, November 2025.

[33] 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.

[34] Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, and Vaibhav Garg. Caraf: crypto agility risk assessment framework. *Journal of Cybersecurity*, 7(1):tyab013, 2021.

[35] 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.

[36] 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.

[37] 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.