POST-QUANTUM CRYPTOGRAPHY MIGRATION STRATEGY

This briefing evaluates two migration strategies for achieving quantum resistance: immediate transition to PQC-only algorithms versus a hybrid classical+PQC approach. While a PQC-only strategy appears to offer a single migration event, it assumes an idealized future where newly-standardised algorithms prove flawless despite limited real-world exposure. A hybrid approach provides defence-in-depth while maintaining cryptographic agility for emerging threats.

The recommendation is to deploy hybrid cryptography as the stable intermediate state, with transition to PQC-only considered only after ten or more years of algorithm maturity and real-world validation.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Table of Contents

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1 Introduction

This briefing evaluates two approaches for achieving quantum-resistant security: an immediate migration to PQC-only algorithms and a hybrid approach that combines classical and post-quantum cryptography. While a PQC-only strategy may appear attractive as a one-time migration, it relies on the assumption that recently standardized post-quantum algorithms will remain secure despite their limited deployment history and relatively short period of cryptographic scrutiny. In contrast, hybrid cryptography provides an additional layer of protection by leveraging the strengths of both classical and post-quantum algorithms, reducing the risks associated with relying exclusively on a new cryptographic paradigm.

A hybrid approach also preserves cryptographic agility, enabling organizations to adapt to future developments, emerging threats, or potential weaknesses discovered in post-quantum algorithms. It allows for a gradual and lower-risk transition to quantum-safe security while maintaining protection against both current and future attack vectors. Therefore, this briefing recommends hybrid cryptography as the preferred intermediate state, with a transition to PQC-only deployments considered only after a sustained period—potentially ten years or more—of real-world validation, operational maturity, and continued cryptographic confidence in PQC algorithms.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2 Background

The Quantum Threat

Cryptographically Relevant Quantum Computers (CRQC) capable of breaking current public-key cryptography are estimated to be ten to fifteen years away, though timelines remain uncertain. However, adversaries are already conducting "harvest now, decrypt later" attacks, capturing encrypted data today with the intention of decrypting it once quantum computers become available. Current widely-deployed algorithms including RSA, Elliptic Curve Cryptography, and Diffie-Hellman key exchange will all be vulnerable to Shor's algorithm running on sufficiently powerful quantum computers.

NIST Post-Quantum Cryptography Standardization

The National Institute of Standards and Technology finalised three post-quantum cryptographic standards in August 2024. FIPS 203 defines ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), FIPS 204 specifies ML-DSA (Module-Lattice-Based Digital Signature Algorithm), and FIPS 205 establishes SLH-DSA (Stateless Hash-Based Digital Signature Algorithm). These standards represent the culmination of an eight-year international competition to identify quantum-resistant cryptographic algorithms. Additional algorithms are expected to be standardized in future rounds as the field continues to mature.

Your Strategic Objective

Organizations seek to avoid multiple cryptographic migrations while ensuring long-term security against both classical and quantum threats. This briefing evaluates which migration strategy best achieves this objective, given the uncertainties inherent in newly-standardised cryptographic algorithms and the evolving threat landscape.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3 PQC-Only Migration

Strategic Description

A PQC-only migration involves direct transition from classical cryptography (RSA and ECC) to NIST-standardised post-quantum algorithms, eliminating classical algorithms entirely from cryptographic infrastructure. This approach represents a clean break with quantum-vulnerable systems and positions the organisation with forward-looking cryptographic capabilities.

Strategic Advantages

Single Migration Event

The most compelling argument for PQC-only migration is the promise of a single planned transition that addresses the quantum threat completely. Once implemented, this strategy eliminates the need to maintain dual algorithm support indefinitely and provides a simplified long-term architecture. From a project management perspective, this appears to align perfectly with the objective to avoid multiple migrations, as it represents one decisive move rather than an incremental approach.

Reduced Operational Complexity

A PQC-only architecture maintains a smaller codebase with fewer algorithms to support, test, and validate. This simplification extends to key management systems, certificate authorities, and cryptographic libraries. The operational overhead is lower than hybrid approaches, as teams need expertise in only one family of algorithms rather than maintaining competency across both classical and post-quantum systems.

Performance Considerations

PQC-only systems offer better performance than hybrid combinations. While post-quantum algorithms are generally slower than their classical counterparts, they remain faster than running both classical and PQC operations in combination. Certificate sizes and bandwidth requirements are also lower than hybrid approaches, though still larger than classical-only systems. For resource-constrained environments or high-throughput applications, these performance characteristics may prove decisive.

Alignment with Forward-Looking Security Posture

This approach eliminates any reliance on algorithms that will eventually become vulnerable to quantum attacks. It aligns with NSA's CNSA 2.0 guidance, which recommends direct transition to post-quantum cryptography rather than hybrid approaches. From a strategic messaging perspective, it demonstrates the organization's commitment to next-generation security capabilities.

Strategic Disadvantages

The Idealized Future Assumption

The fundamental weakness of PQC-only migration is that its success depends on an idealized future that may not materialize. This strategy requires that NIST-selected

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

algorithms contain no exploitable cryptanalytic weaknesses, that no implementation vulnerabilities emerge through side-channel attacks or fault injection, that the underlying mathematical foundations remain sound, that no classical algorithmic breakthroughs reduce security margins, and that the standards themselves require no major revision.

Each of these assumptions carries significant risk. Cryptographic systems rarely prove flawless upon initial deployment. The history of cryptography is one of continuous refinement through adversarial discovery, not of perfect prediction through standardization processes. Betting your organization's security on the assumption that this time will be different represents a considerable leap of faith.

Historical Precedent Argues Against Confidence

Recent history provides sobering examples of post-quantum algorithm failures. Rainbow, a NIST Round 4 finalist, was broken in 2022 shortly after advancing in the competition. SIKE, another Round 4 finalist, suffered a similar fate the same year. Even the selected algorithms have experienced concerning developments, with multiple side-channel and implementation attacks discovered against ML-KEM and ML-DSA implementations.

These algorithms have undergone less than ten years of intensive cryptanalysis, compared to the thirty to forty years of scrutiny that RSA and ECC have survived. While this does not prove they are insecure, it does mean we lack the confidence that comes from decades of failed attack attempts. The cryptographic community's understanding of lattice-based, code-based, and hash-based security is still maturing.

Absence of Fallback Position

Perhaps most critically, a PQC-only approach provides no fallback position if problems emerge. **Should a selected algorithm prove vulnerable, organizations face emergency migration under pressure—precisely the scenario you are trying to avoid**. The goal of avoiding multiple migrations fails catastrophically if PQC proves vulnerable, as you would then require an unplanned migration to alternative algorithms or back to classical systems while quantum threats loom.

This represents a single point of failure in your security architecture. Unlike hybrid approaches where either component can maintain security if the other fails, PQC-only creates a brittle system where a single cryptanalytic breakthrough compromises your entire infrastructure.

Asymmetric Timeline Risk

A frequently overlooked risk is the asymmetric timeline between quantum computing development and potential PQC algorithm failures. Post-quantum algorithms could fail before quantum computers break classical cryptography. Classical cryptanalysis advances much faster than quantum hardware development. If a mathematical or algorithmic breakthrough undermines PQC in the next five years while quantum computers remain fifteen years away, a PQC-only organization would face a window of vulnerability where neither the old system (already migrated away from) nor the new system (now broken) protects them.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4 Hybrid Classical + PQC Approach

Strategic Description

A hybrid approach combines classical algorithms (RSA or ECC) with post-quantum algorithms such that security requires breaking both components simultaneously. An attacker must solve both the classical mathematical problems (factoring or discrete logarithm) and the post-quantum problems (lattice-based, code-based, or hash-based), making the system secure as long as either component remains unbroken.

Strategic Advantages

Defence in Depth Through Independent Hard Problems

The fundamental strength of hybrid cryptography is that it provides defence in depth through mathematically independent hard problems. Security is maintained if either component remains secure, meaning an adversary must achieve two independent cryptanalytic breakthroughs rather than one, making this more than simply redundancy—it is true defence against divergent threat scenarios. If quantum computers arrive before PQC algorithms fail, the PQC component protects you. If PQC algorithms fail before quantum computers mature, the classical component protects you. Only the simultaneous failure of both systems compromises security.

This approach maximizes the security margin during the uncertain transition period. It acknowledges that we cannot predict with confidence which threat will materialize first—quantum computing capabilities or PQC algorithm vulnerabilities—and protects against both scenarios.

Cryptographic Agility for Evolving Threats

Hybrid systems provide genuine cryptographic agility. If vulnerabilities emerge in PQC algorithms, you can swap to alternative post-quantum algorithms while maintaining the classical component, avoiding complete infrastructure migration. This provides a graceful evolution path rather than forcing emergency responses. Similarly, as quantum computing capabilities evolve, you can strengthen or replace the classical component while the PQC layer maintains security.

This agility is not theoretical—it is precisely how the cryptographic community has managed algorithm transitions historically. Systems evolve incrementally rather than through wholesale replacement, and hybrid architectures enable this evolutionary approach to continue into the post-quantum era.

Industry Consensus and Standards Support

The hybrid approach represents the **consensus position of the broader cryptographic community**. NIST's guidance explicitly supports hybrid cryptography during the transition period. The German Federal Office for Information Security (BSI) **explicitly recommends hybrid approaches in their technical guidelines**. The European Telecommunications Standards Institute (ETSI) has published hybrid standards. Major cloud service providers including AWS, Google Cloud, and Cloudflare are deploying hybrid

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

TLS implementations. The Internet Engineering Task Force is developing hybrid standards for TLS, SSH, and IPsec.

This consensus emerged from careful risk analysis by organizations with deep cryptographic expertise and operational responsibility for protecting critical infrastructure. While the NSA's CNSA 2.0 takes a different position, it represents a minority view. **The weight of expert opinion favors hybrid approaches precisely because they manage risk more effectively** during periods of algorithmic uncertainty.

Realistic Risk Management Philosophy

Hybrid cryptography embodies a philosophy of realistic risk management. It acknowledges that we cannot predict which cryptographic systems will fail first, that new algorithms require time to prove themselves through adversarial testing, and that security systems must be designed to survive partial failures. This is fundamentally different from the optimistic planning inherent in PQC-only approaches.

By maintaining proven security mechanisms (classical algorithms with decades of scrutiny) while adding quantum resistance (PQC algorithms), hybrid systems balance innovation with prudence. Organisations can adopt quantum-resistant capabilities without betting their entire security posture on algorithms that have been publicly available for less than a decade.

Compliance Flexibility

Hybrid approaches provide maximum flexibility for evolving compliance requirements. If future regulations require maintaining classical algorithms for interoperability or backwards compatibility, hybrid systems are already compliant. If regulations mandate PQC-only, the transition path from hybrid is straightforward and low-risk. This hedges against regulatory uncertainty in an area where standards and requirements are still rapidly evolving.

Strategic Disadvantages

Performance and Bandwidth Overhead

Hybrid systems incur computational overhead from performing both classical and post-quantum operations. Benchmarks typically show five to ten percent increased processing time for cryptographic operations. Certificate and key sizes increase, leading to higher bandwidth consumption—particularly relevant for resource-constrained IoT devices or high-frequency trading systems where microseconds matter. Power consumption rises marginally, which may concern mobile or edge computing deployments.

However, these performance penalties must be evaluated against the risk reduction provided. For most enterprise applications, a ten percent performance overhead is manageable and acceptable given the security benefits. The performance argument against hybrid is strongest in specific use cases with extreme performance requirements, not as a general principle.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Implementation Complexity

Maintaining two algorithm families increases implementation complexity. Development teams must maintain expertise in both classical and post-quantum cryptography. Key management systems must handle both key types. The codebase expands, creating a larger attack surface and more opportunities for implementation errors. Testing and validation processes become more elaborate.

This complexity is real but manageable. Organisations already maintain complex cryptographic infrastructures supporting multiple algorithms, cipher suites, and key types. Hybrid approaches extend existing complexity rather than introducing entirely new categories of challenge. The operational complexity of hybrid systems is significantly less than the complexity of emergency migration following an algorithm failure.

Perceived Need for Multiple Migrations

Hybrid approaches appear to require two migration events: an initial migration to hybrid, and an eventual migration to PQC-only. This seems to conflict directly with the objective to avoid multiple migrations. However, this perception misunderstands the risk profile and timeline. The second migration (from hybrid to PQC-only) is optional and can be indefinitely deferred if hybrid continues to meet security requirements. More importantly, it becomes a low-risk planned evolution rather than an emergency response, which is the true goal when seeking to avoid disruptive migrations.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5 Risk Anaylsis

The Multiple Migrations Paradox

Organizations' concern about avoiding multiple migrations is well-founded, but it is essential to understand what actually minimises migration risk. A PQC-only approach avoids multiple migrations only if nothing goes wrong—only if the idealized future materialises and PQC algorithms prove completely robust. If PQC algorithms fail, you face exactly the emergency migration scenario you are trying to avoid, and potentially a more difficult one because you have no fallback position.

Hybrid cryptography paradoxically offers the more stable path to avoiding forced migrations. You conduct one planned migration to hybrid, which then serves as a stable security posture regardless of which threat materialises first. If PQC algorithms require replacement, you swap them within the hybrid framework—a much smaller operation than complete infrastructure migration. If PQC algorithms prove robust over a decade or more, transitioning from hybrid to PQC-only becomes a low-risk optional enhancement rather than a forced march.

The migration scenarios illustrate this clearly. The PQC-only path proceeds from classical cryptography to PQC-only, and then if PQC fails, requires emergency migration to an uncertain destination. The hybrid path proceeds from classical to hybrid, and then if PQC fails, allows you to swap PQC algorithms while maintaining the classical security layer. If PQC matures successfully, you can gradually transition to PQC-only at your discretion.

Asymmetric Risk Profile

The risk profiles of these two approaches are fundamentally asymmetric. In a PQC-only architecture, an algorithm break is catastrophic—it eliminates your security and requires emergency response. In a hybrid architecture, an algorithm break in either component is manageable—the other component maintains security while you implement a planned response.

Consider the timeline uncertainty. Quantum computing may arrive in ten years or twenty-five years. PQC algorithms may remain secure for decades or may experience major breaks within five years. We cannot predict these timelines with confidence. Hybrid approaches remain secure across all reasonable scenarios. PQC-only approaches create vulnerability windows if the timelines diverge in unfortunate ways.

The performance overhead of hybrid (five to ten percent) is modest and predictable. The operational complexity of hybrid is manageable with proper planning. These disadvantages are concrete and bounded. The risks of PQC-only—catastrophic algorithm failure requiring emergency migration—are potentially severe and difficult to manage when they materialise.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Timeline for Algorithm Maturity

A realistic assessment of algorithm maturity timelines is essential for this decision. The PQC standards were finalized in August 2024. The period from 2025 to 2027 will see initial deployments and early vulnerability discovery as implementation flaws and side-channel attacks are identified. From 2028 to 2030, wider adoption will drive implementation hardening and additional scrutiny. Only in the period from 2030 to 2035 will these algorithms accumulate sufficient real-world adversarial exposure to assess their robustness with genuine confidence.

This suggests that hybrid cryptography should be maintained for at least a decade before considering transition to PQC-only. After ten to fifteen years without major algorithm breaks, after implementations have been hardened against side-channel attacks, after the cryptographic community has thoroughly explored the mathematical foundations, then and only then can organizations reasonably consider PQC-only as a stable endpoint.

The quantum threat timeline of ten to fifteen years (or potentially longer) provides exactly this window. Hybrid cryptography can be maintained throughout this period, allowing PQC algorithms to mature while quantum capabilities develop. The timing works favourably for a patient, risk-managed approach.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

6 Recommendation

Deploy Hybrid Classical+PQC Cryptography

This briefing recommends deploying hybrid classical+PQC cryptography as the strategic migration path. This recommendation rests on five core arguments.

First, hybrid cryptography minimises actual migration risk by providing security regardless of which threat materializes first—quantum computing or classical cryptanalysis of PQC algorithms. It is the only approach that protects against timeline divergence where PQC fails before classical cryptography is threatened by quantum computers.

Second, hybrid approaches actually address the goal to avoid multiple migrations more effectively than PQC-only. Hybrid represents a stable endpoint that can be maintained indefinitely if needed, with optional evolution to PQC-only only after algorithms prove themselves. PQC-only creates risk of forced emergency migration if algorithms fail.

Third, the hybrid approach aligns with industry best practice and the consensus of the cryptographic community. The majority of security agencies (excluding NSA), standards bodies, and major cloud providers are deploying hybrid solutions based on their assessment of the risk landscape.

Fourth, hybrid cryptography manages uncertainty appropriately. It acknowledges that we cannot predict which cryptographic systems will fail first and designs for resilience rather than optimality. This is prudent engineering in the face of genuine uncertainty about both quantum computing timelines and PQC algorithm robustness.

Fifth, hybrid maintains cryptographic agility, allowing algorithm failures to be addressed incrementally through planned evolution rather than through emergency responses that compromise security during transition periods.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Conclusion

The choice between PQC-only and hybrid migration strategies is not primarily a technical decision—it is a risk management decision about how to navigate genuine uncertainty. PQC-only migration represents a bet on an idealized future where newly-standardised algorithms prove flawless despite limited real-world exposure. Cryptographic history demonstrates that security systems evolve through adversarial discovery, not through perfect prediction. Algorithms require years or decades of scrutiny to establish genuine confidence in their robustness.

Hybrid cryptography acknowledges this reality. It provides defence-in-depth while maintaining the cryptographic agility necessary to respond to emerging threats, whether from quantum computers or from classical cryptanalysis. For an organisation seeking to avoid multiple disruptive migrations, hybrid cryptography paradoxically offers the most stable path forward precisely because it remains secure across all reasonable scenarios regarding quantum computing timelines and PQC algorithm robustness.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Disclaimer

This document does not represent the opinion of the European Union or European Commission, and neither the European Union nor the granting authority can be held responsible for any use that might be made of its content.

Neither the Q-PREP consortium as a whole, nor a certain party of the Q-PREP consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk and does not accept any liability for loss or damage suffered by any person using this information.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE