Technology & Architecture

By Tooba Qasim

Why Post-Quantum Cryptography Changes More Than Just Algorithms

When organisations first hear about post-quantum cryptography, the instinctive reaction is often technical and narrow: *"We'll upgrade our encryption libraries when the time comes."*

That reaction is understandable but it misses the bigger picture.

Post-quantum cryptography does not live in isolation. It sits inside architectures that have evolved over decades, layered across networks, applications, identities, cloud platforms, and operational processes. Once you look closely, it becomes clear that PQC is not a simple swap of algorithms. It is an architectural change.

This article explains where cryptography actually lives in modern systems, how PQC affects those layers and why hybrid cryptography plays such a critical role during the transition.

Cryptography Is Everywhere, Even Where You Don't Expect It

In modern digital environments, cryptography is not a single component. It is embedded across almost every technical layer.

When you open a website, **Transport Layer Security (TLS)** encrypts traffic between your browser and the server. When a service authenticates a user or another service, **certificates and keys** validate identities. When teams connect remote workers or data centres, **VPNs** establish secure tunnels. APIs rely on cryptographic tokens, cloud platforms manage keys behind the scenes and identity systems use cryptography to bind trust to users, devices and services.

Most organisations don't consciously design "cryptographic architecture." Instead, cryptography accumulates organically as systems grow, vendors change and new platforms are added. Over time, this creates a web of dependencies, some visible many hidden.

PQC touches all of these places.

Why Post-Quantum Cryptography Is Architecturally Different

Classical cryptographic algorithms such as RSA and elliptic-curve cryptography are compact and well-understood. Keys are relatively small, handshakes are fast and protocols have been tuned around their performance characteristics.

Post-quantum algorithms behave differently.

Many PQC schemes use **larger keys and signatures**, sometimes by an order of magnitude. Handshakes may involve more data being exchanged. Memory usage and network overhead can increase, especially in constrained environments.

This does not mean PQC is impractical, it means systems need to be **architecturally aware** of these differences.

A cryptographic library upgrade might work in a test environment but fail under real-world load if the surrounding architecture was never designed to handle larger messages, slower handshakes or additional negotiation steps.

TLS and Secure Communications

TLS is one of the first places organisations encounter PQC in practice.

Modern TLS handshakes rely on public-key cryptography to establish shared secrets. With PQC, those key exchanges change. During the transition, most implementations use **hybrid key exchange**, combining a classical algorithm with a post-quantum one in the same handshake.

From an architectural perspective, this affects load balancers, reverse proxies, API gateways and any system that terminates TLS. Some older devices or embedded systems may not support updated handshake sizes or algorithm negotiation, even if the application itself is compatible.

This is why PQC readiness often starts with **network architecture reviews**, not application code.

PKI, Certificates and Trust Chains

Public Key Infrastructure (PKI) is one of the most complex and least visible cryptographic systems in an organisation.

Certificates authenticate servers, devices, users and software updates. Certificate chains often involve internal certificate authorities, third-party trust anchors and long-lived embedded certificates in hardware or firmware.

PQC directly impacts PKI because **digital signatures change**. Certificate sizes grow, signing algorithms evolve and validation logic must be updated across systems that may not have been touched in years.

Architecturally, this raises important questions: where certificates are generated, how they are distributed, how long they live,and how trust chains are validated across environments.

If PKI is fragmented or poorly documented, PQC migration becomes significantly harder.

VPNs, Remote Access and Network Segmentation

VPNs are another layer where cryptography is deeply embedded.

Key exchange protocols such as **Internet Key Exchange (IKE)** rely on public-key algorithms to authenticate endpoints and derive session keys. Introducing PQC into these systems affects not only cryptographic libraries but also appliance compatibility, performance tuning, and interoperability between vendors.

For organisations with hybrid or multi-cloud networks, VPN architectures often span on-premise systems, cloud gateways and partner environments. A partial upgrade can easily lead to mismatches or insecure fallbacks if not carefully planned.

This is why PQC planning must consider **end-to-end network architecture** not just individual components.

APIs, Microservices and Internal Trust

Inside modern organisations, APIs and microservices rely heavily on cryptography for authentication and authorisation. Tokens, service identities and mutual TLS connections all depend on cryptographic primitives.

As systems scale, these internal trust relationships multiply. A single application may depend on dozens of cryptographically authenticated services, each with its own lifecycle and ownership.

PQC does not change the *idea* of zero-trust or service-to-service authentication, but it does affect how identities are represented, how keys are managed and how trust is rotated over

time. Architects need to understand where cryptographic trust is enforced and how flexible those mechanisms are.

Cloud Platforms and Managed Cryptography

Cloud providers abstract much of cryptography away from users. Key management services, managed TLS endpoints and identity platforms handle cryptographic operations behind the scenes. This abstraction is helpful but it also introduces dependencies.

Organisations adopting PQC will need to align their architecture with **cloud provider roadmaps**, understand which services will support post-quantum algorithms first and where hybrid approaches will be used automatically versus requiring configuration changes.

Architectural visibility remains essential, even when cryptography is "managed."

Why Hybrid Cryptography Is Architecturally Essential

Hybrid cryptography is not just a cryptographic compromise; it is an architectural safety mechanism.

By combining classical and post-quantum algorithms, hybrid approaches ensure that systems remain secure even if one algorithm is later found to be weaker than expected. This layered approach mirrors established architectural principles such as defence-in-depth and redundancy.

From a system design perspective, hybrid cryptography buys time. It allows organisations to upgrade infrastructure gradually, test performance impacts and maintain interoperability while standards and implementations mature.

Trying to leap directly to "pure PQC everywhere" is neither realistic nor necessary.

A Simple Way to Visualise the Impact

If you want a mental model, imagine cryptography as a **horizontal layer** running through your architecture rather than a single vertical component.

From the browser to the API gateway, from identity systems to databases, from on-premise networks to cloud services, cryptography binds everything together. Changing it affects how those layers interact.

The Architectural Takeaway

Post-quantum cryptography forces organisations to confront something many have postponed for years: **understanding where and how cryptography actually operates in their systems**.

The organisations that succeed in this transition will not be the ones with the fastest algorithm upgrades. They will be the ones with clear architectural visibility, flexible trust models and systems designed to evolve.

In the preparation phase, technology and architecture are not about solving everything at once. They are about building a structure that can change safely because in the post-quantum era, change is the only constant.