Migration to Post-Quantum Cryptography

Kris Kwiatkowski

No Institute Given

The global internet security ecosystem is preparing for one of its biggest shifts in decades: the migration from traditional cryptographic algorithms to post-quantum cryptography. Quantum computing may still be years away from breaking widely deployed algorithms, but the "harvest-now, decrypt-later" (HNDL) threat makes planning and transitioning urgent. Sensitive data encrypted today could be collected and decrypted in the future once cryptographically relevant quantum computers (CRQCs) arrive.

Here are some thoughts on the migration.

1 Why Start the Migration?

You don't want to be caught off guard when quantum computers become capable of breaking current cryptographic standards. The migration process is complex and time-consuming, often taking several years to complete. Organizations must first evaluate when and how to begin, considering factors such as:

1. **Data lifetime** – how long the information you protect needs to remain confidential.
2. **Migration complexity** – how much effort is required across systems, hardware, and vendors.
3. **Quantum threat timeline** – how soon a CRQC could become practical.

Even without immediate existential risk, planning and testing today ensures you aren't forced into a rushed, high-cost migration tomorrow. More complicated systems, such as old, small embedded devices, may take years to update, replace, or ideally redesign with PQC in mind.

Starting this transition early is definitely a good idea, because migration can be complex and time-consuming. But without panic and feeling pressured to start immediately. Be deliberate when selecting products and suppliers - this technology is still maturing and not yet fully commoditized, which means higher costs and potential risks. Open-source solutions can help mitigate some of these challenges, though they come with their own uncertainties. Proprietary options may provide stronger support and stability but can also create dependency on specific vendors and ecosystems. In short, try hard to avoid the "sell-now, forget-later" mindset - this remains a developing field with trade-offs, uncertainties, and costs that must be carefully balanced.

2 Key Exchange in TLS: The Most Urgent Step

TLS key exchange is the top priority for PQC migration. If session keys are negotiated using quantum-vulnerable algorithms, future quantum computers could decrypt recorded traffic. To mitigate this, PQ/T hybrid key exchange is recommended during the transition. These approaches combine at least one post-quantum and one classical algorithm, so security is maintained as long as one remains unbroken. Hybrid KEMs are also easier to roll out than post-quantum signatures, since they are ephemeral and not linked to long-term identity.

As PQC matures, hybrid KEMs will become less important, and eventually only the post-quantum algorithm will be needed.

The IETF began work on standardizing post-quantum key exchange for TLS in 2019, after a key workshop at Mozilla's Mountain View offices and early Google-led experiments. This resulted in a framework for new key exchange methods, and the TLS Post-Quantum Experiment showed hybrid KEMs in action.

The first widely adopted Internet draft for hybrid key exchange in TLS is now close to completion. This draft and its extension have become the de facto standard for modern TLS, with implementations already available in OpenSSL, NGINX, and AWS's AWS-LC library, and are already widely deployed. Jan Schuman from Akamai has a great post on sites already using PQC.

TLS is not the only protocol that needs quantum-safe key exchange. For this reason, there is also an effort to standardize a more generic approach to hybrid KEM constructions for broader use.

3 Digital Signatures: Important, But Less Urgent

Digital signatures remain a vital component of cryptographic protocols, ensuring authenticity, integrity, and non-repudiation. As such, post-quantum digital signature schemes are necessary for a future-proof internet infrastructure. However, the urgency to deploy them is relatively lower compared to key encapsulation mechanisms (KEMs).

Unlike key exchange, authentication cannot be broken retrospectively, meaning quantum-safe signatures are only needed once cryptanalytically relevant quantum computers become available. As a result, the migration to post-quantum digital signatures is less time-sensitive than for KEMs, allowing for a more deliberate and carefully planned transition. Since post-quantum signature schemes often involve larger keys and signatures, greater computational overhead, and increased implementation complexity, their deployment may incur higher costs - reinforcing the importance of keeping the migration - —as simple and efficient as possible.

Determining whether and when to adopt PQC certificates or PQ/T hybrid schemes may depend on several factors, such as:

– Frequency and duration of system upgrades

– Operational flexibility to enable or disable algorithms

Deployments with limited flexibility (e.g., embedded systems) benefit significantly from PQ/T hybrid signatures. This approach mitigates the risks associated with delays in transitioning to PQC and provides an immediate safeguard against zero-day vulnerabilities.

While hybrid constructs may seem plausible for long-term security, they also introduce complexity, potential performance overhead, and long-term implications:

– The number of possible hybrid combinations leads to interoperability challenges and increased implementation burden.
– If one scheme is compromised, forgery is only a concern while the corresponding public key remains trusted.
– Long-term protection through hybrids may be limited in practice due to standard key management practices.

There is another risk related to the potential misuse of PQ/T hybrid signatures. Consider this: a deployment may use hybrid signatures to facilitate migration, resulting in a mix of devices - some aware of PQ schemes and some not. Devices unaware of PQ schemes may continue to validate only the traditional signature, while those aware of PQ schemes may validate both signatures. A deployment might continue this approach even after the traditional algorithm has been broken. While this may simplify operations by avoiding re-provisioning of trust anchors, it introduces a significant risk. A CRQC could forge the broken traditional signature component over a message, then combine it with the valid post-quantum component to produce a new composite signature that verifies successfully. This underscores the critical need to retire hybrid certificates containing broken algorithms once CRQCs become available (and always validate both components of a hybrid signature).

The IETF has many experts working on this topic. For example, draft-ietf-lamps-pq-composite-sigs describes how to create and verify composite signatures that combine a post-quantum signature with a classical signature.

Nevertheless, hybrid signatures remain complicated and may not be suitable for all scenarios. Fortunately, they are only needed once quantum computers are capable of breaking current signature algorithms. So, we still have some time to make the authentication migration as smooth as possible.

4 Infrastructure Costs: What to Expect

This topic is both important and frequently overlooked. Migrating to post-quantum cryptography (PQC) often requires significant updates to existing infrastructure. Careful planning and budgeting are essential, as costs can arise in multiple areas.

The first step is discovery - building a comprehensive inventory of all cryptographic assets and where they are used. This process may require specialized tools and can itself be resource-intensive.

Another major factor is whether updates can be delivered through software patches or require new hardware. For some systems, particularly constrained or niche devices, supporting PQC may require custom development or even physical replacement. Engaging with vendors early is critical to understand available options and associated costs.

Key infrastructure components that will need attention include:

- Network protocols – TLS, SSH, and QUIC must be adapted to handle larger PQC artifacts. While PQC KEMs such as ML-KEM often perform competitively in handshakes, their larger message sizes can increase bandwidth use, add round trips, or introduce latency.
- Message processing – PQC signature algorithms typically process entire messages rather than digests. This can hurt performance in systems like HSMs that rely on streaming data, unless applications adopt pre-hashing or streaming-friendly designs.
- PKI systems – Certificate Authorities (CAs), certificate formats, and trust anchors must all evolve to support PQC. Hybrid certificate formats can ease transition but also add complexity and operational overhead.
- Constrained devices – Long-lived systems (e.g., satellites, industrial controllers, smart meters) are especially difficult to update. Limited memory and compute resources may force costly redesigns or replacements, and in-field updates can be logistically challenging.
- Hybrid approaches, while helpful for resilience during the transition, can add two layers of cost: first to support dual algorithms (certificates, key management, validation), and later to migrate again once hybrids are no longer needed. In some environments, this two-step process is more expensive than planning a direct migration to PQC at the right moment.
- Training and Awareness: Ensuring that staff are knowledgeable about PQC concepts, like KPIs provided by PQC implementations and impact on performance, familiar with tradeoffs of PQ/T hybrid schemes and their implications on migration process are essential. This may involve training programs, workshops, or hiring specialized personnel, all of which contribute to the overall cost.

Long-term savings come from embracing cryptographic agility: designing systems that can switch algorithms without major architectural changes. This reduces the cost of future transitions - but achieving true agility requires upfront investment in both design and standardization.

5 Final Thoughts

Migrating to post-quantum cryptography is not a single upgrade — it is a long-term process. As mentioned at the beginning of this article, starting this transition early is definitely a good idea.

It is worth recalling that the first IETF draft proposing a PQ/T hybrid key exchange for TLS was published back in 2019 (I agree, it wasn't serious proposal at the time), nevertheless we are now in 2025, and only recently have PQ/T hybrid standards been finalized by the IETF and started to see adoption by major browsers. That is six years for a single - and relatively simple - use case: key exchange in TLS.

When it comes to digital signatures, the migration will be significantly more complex and time-consuming. Based on current timelines and projections for quantum computing, cryptographically relevant quantum computers are expected to emerge by the end of the next decade. This leaves less than ten years to finalize standards and initiate large-scale migration. Not in TLS, but everywhere. Given that such migration efforts typically span several years, it is clear that we are already behind schedule.

The situation today, however, is quite different from 2019: the first PQC algorithms have been standardized, and there is far greater motivation and momentum to move forward. Nevertheless, much remains to be done. The key is to plan for agility and actively align with emerging standards. Going back to the beginning of this article: don't wait until the last minute, but also don't rush into unproven solutions. Balance risk, cost, and operational complexity carefully.

The transition will be uneven: some systems will adopt hybrids, some will wait for pure PQC. Constrained devices may require tailored strategies and highly optimized implementations to match the performance and resource utilization of traditional algorithms. But the direction is clear: a future-proof Internet must stay safe!

Ongoing work in the IETF focuses on general guidance for migration to PQC as well as guidance for constrained devices. Feel free to join the discussions in the PQUIP Working Group.