ETSI/IQC Quantum Safe Cryptography Conference 2026

Our Quantum-Safe Infrastructure Migration

Presented by: Shane Kelly

17/06/2026

What did we do?

digicert®

We focused on the big stuff

TLS

- TLS 1.2 to TLS 1.3
- Added X25519MLKEM768 as a key_share option.
- Update *almost* all of our connections. We didn't get all of them and that's Ok for now.

HSMs

- We updated some of our HSMs. And by update, I mean purchase new ones.
- We wrote an abstraction layer to interface with multiple HSM vendors.
- Update the plumbing so customers could use the new quantum-safe algorithms.

Private PKI

- Get ML-DSA into our private PKI offerings.
- Make sure the software in our private PKI instances could support ML-DSA (a lot couldn't).
- Deploy ML-DSA certs.

Challenges.

digicert®

Vendors

That vendors represent the greatest challenge isn't too surprising. The few quantum-safe issues we had with vendors were.

- We did have to move away from one vendor to another that had better quantum-safe timelines.
- Our WAF took about 7 months to onboard us to a beta. It wasn't 7 months of quantum-safe work, the challenge was the project manager left the company and a new one had to be onboarded.
- Our load balancers needed to be updated to a different version for quantum-safe support. A version that our current (at the time) support contract didn't cover. It had to be renegotiated.
- Bought new HSMs and had to write new interface code for them. There were also versioning issues around FIPS that caused some headaches.

Impact!

digicert®

Very little customer impact.

Of the ~200,000 customers that have connected to our endpoints, we've had only one with issues. Their TLS software can't handle endpoints that support TLS 1.3. The failure happened before we enabled quantum-safe key exchange so it's not a problem directly related to the quantum-safe transition.

TLS 1.3 endpoints with x25519mlkem768 haven't caused issues for other customers.

Internal impact has been minimal.

- Internally there haven't been any negative quantum-safe related impact outside of the costs and sprint cycles used for development.
- No service disruptions or software rollbacks have been needed that can be attributed to using quantum-safe algorithms.
- Regular software development problems were encountered, primarily when integrating the new HSMs.
- So far, the larger sizes of quantum-safe algorithms haven't caused issues for us.

How much did it cost?

digicert®

Less than expected

The primary cost was HSMs.

We had to renegotiate our load balancer contract to cover the version we needed. The new version doesn't seem directly tied to quantum-safe support and there was no increase in cost. There was a time delay and person cost associated with this.

For teams that worked on quantum-safe projects there was an increased workload, this was especially true for the HSM integration.

To date we've hired 3 people specifically for quantum-safe initiatives.

What did we learn?

digicert®

The technology is ready.

Library support, technical standard support, and low-level primitives are ready to go.

Be specific when talking about the technology you need. Asking for x25519mlkem768 as a TLS 1.3 key share is going to get your project running faster than asking about quantum-safe options.

This is mostly a software development issue.

Good software development practices give you quantum-safety.

Major Versions

- Not just patches and minor updates.
- Includes the ability to update the operating system.
- It is fairly common for minor updates to work smoothly, the major, API changing, updates are more difficult to manage.

Not Just Crypto

- It's not going to only be crypto that needs updating.
- The software that relies on the crypto may also need to be updated.
- And up the chain…

Dev Pipelines

- Reliable release and rollback procedures.
- Good for development anyway.
- Updating becomes easy since breaks can quickly be reverted.

HSMs will be a big focus.

Unsurprisingly.

Integration Work	HSMs take work to get integrated. This is heightened by the fact that the new NIST algorithms have extra options (ctx, Hash vs Pure) that need to be considered.
Cost	It looks like the primary cost for PQC transitions will be hardware.
Security	We have to discuss how HSMs fit in our security models and whether updating HSM firmware will be enough to provide the security expected by our customers. At the moment, new ones are needed for simplicity.

digicert®

www.digicert.com