
PQ Auth for the Web

— IAB pqws workshop 2026 —

[Home](#) > [Innovation & AI](#) > [Technology](#) > [Safety & Security](#)

Quantum frontiers may be closer than they appear

Mar 25, 2026

1 min read

We're setting a timeline for post-quantum cryptography migration to 2029.

Heather Adkins
VP, Security Engineering

Sophie Schmieg
Senior Staff Cryptography
Engineer

🔗 Share



Home > Innovation & AI > Technology > Safety & Security

Quantum frontiers may be closer than they appear

Mar 25, 2026

1 min read

We're setting a timeline for post-quantum cryptography migration to 2029.

"Google's introducing a 2029 timeline to secure the quantum era with post-quantum cryptography (PQC) migration."

Heather Adkins

VP, Security En

Sophie Schmiege

Product Lead

Share



HTTPS server authentication in Chrome

Chrome root store

- Trusted by default

- Managed by the Chrome Root Program

- Transparency requirement since 2018, currently CT

User-added roots

- Managed by user, enterprise administrator, etc.

- Deployment-specific requirements

Post-quantum HTTPS server authentication

Chrome root store

Transparency adds extra challenges $\Rightarrow$ Merkle Tree Certificates (MTCs)

Progress in PLANTS $\Rightarrow$ Stable deployment target and PKIX OIDs in draft-07

Expect to have CAs and client support early 2027

User-added roots

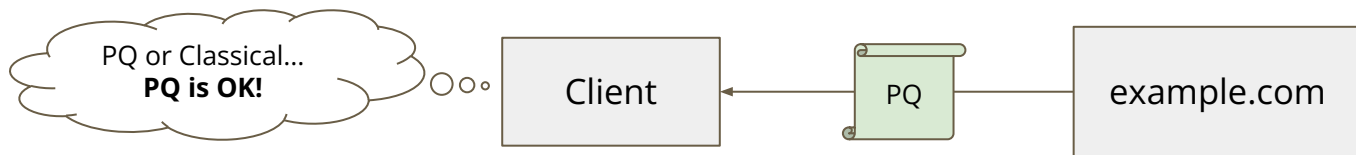
Chrome shipped RFC 9881 and draft-ietf-tls-mldsa in June 2026

Expect to eventually support user-added MTC roots too

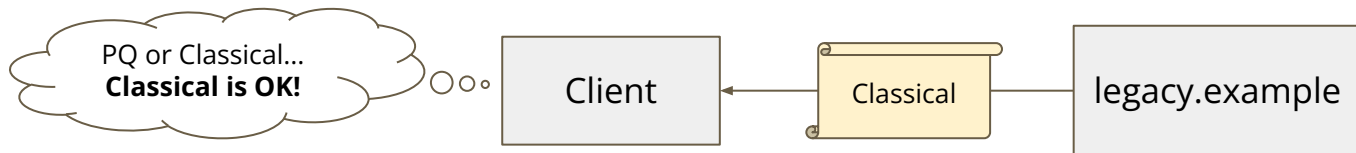
Post-quantum *or* classical

In 2027, Chrome will *support* post-quantum certificates without *requiring* them

Servers can migrate to post-quantum



Legacy servers still work

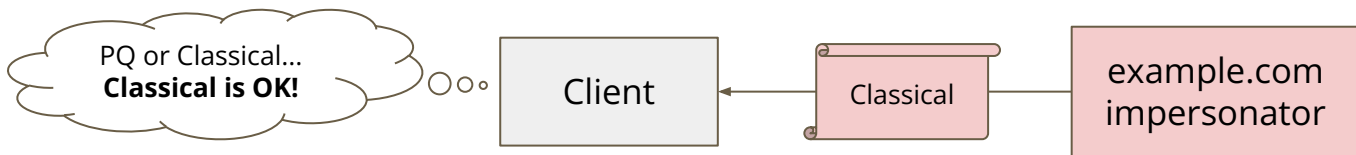


But is this PQ-secure?

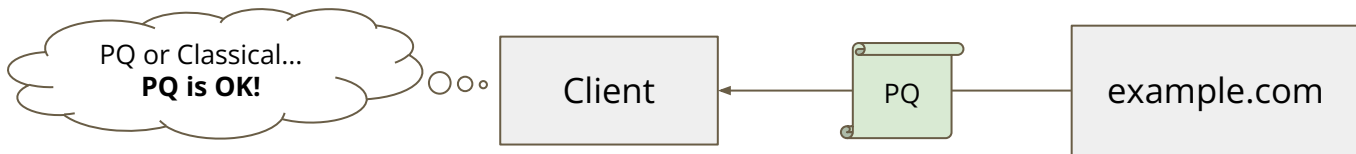
No

Attacker picks the certificate

If Chrome accepts **any classical CA**, the attacker can forge a classical certificate for **any server**



Whether the legitimate certificate uses this CA *does not change this attack*



To protect *any* servers, *all*
classical CAs must be
removed from PQ clients

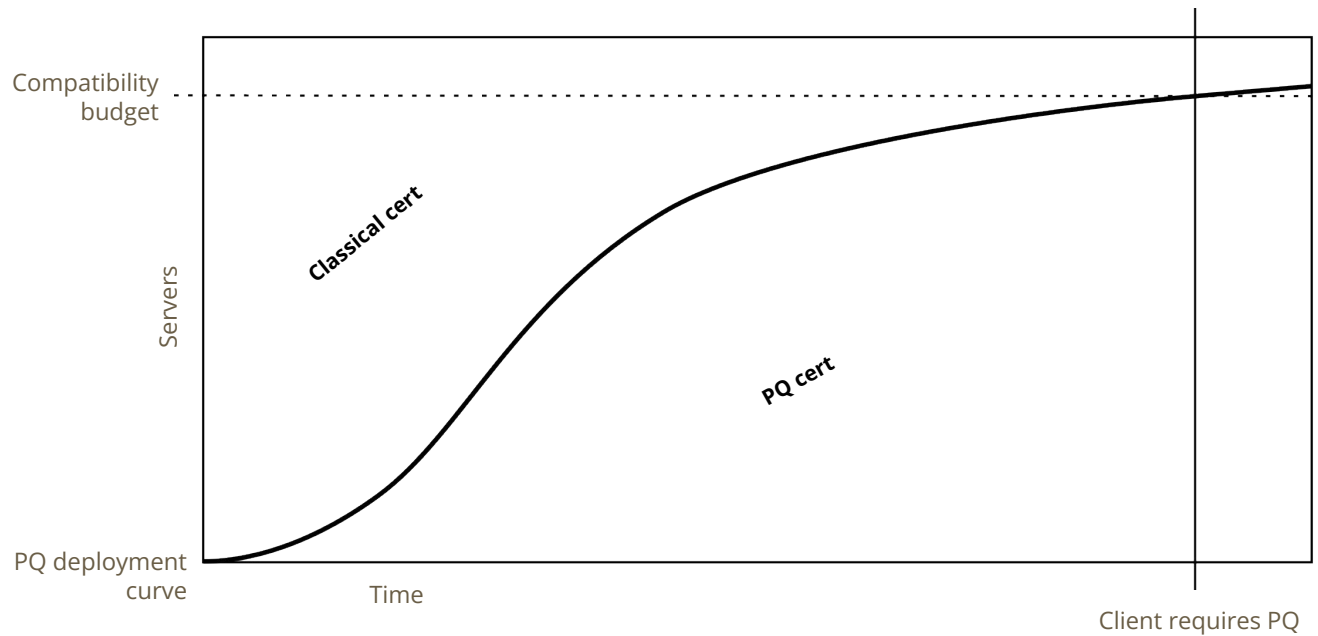
But legacy servers aren't going away

Legacy systems predate PQ and *do not support PQ certificates*. We *cannot fix them* without updating them.

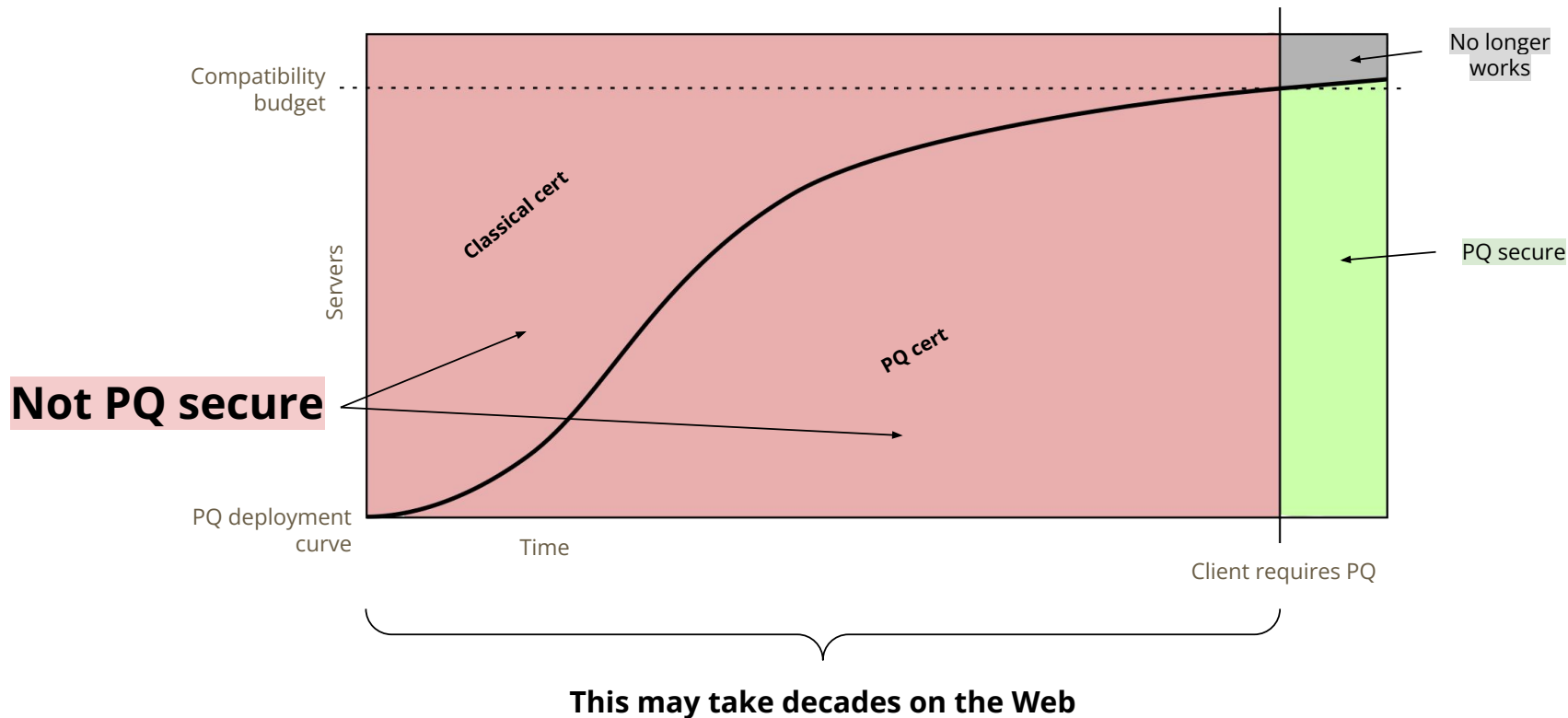
The Web is big. Lots of sites will not be updated promptly.

Legacy sites still matter to users. We can't just refuse to connect them.

PQ deployment curve



Downgrade is possible until client enforcement



Split the transition in two?

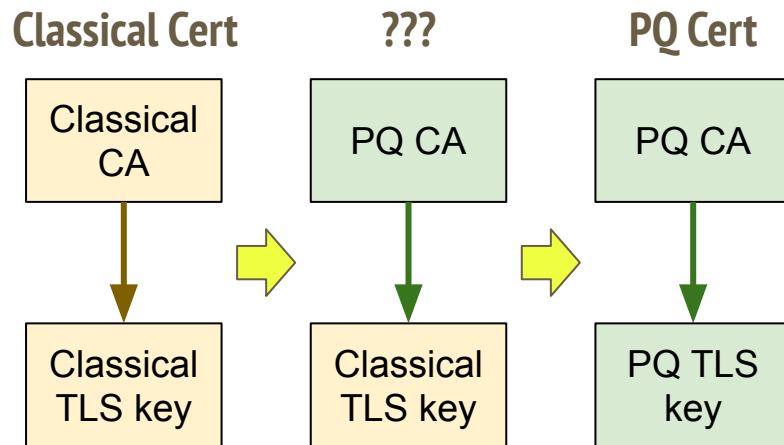
A certificate involves *two* keys: CA's key, and server TLS key

Switching TLS key requires **per-server** work

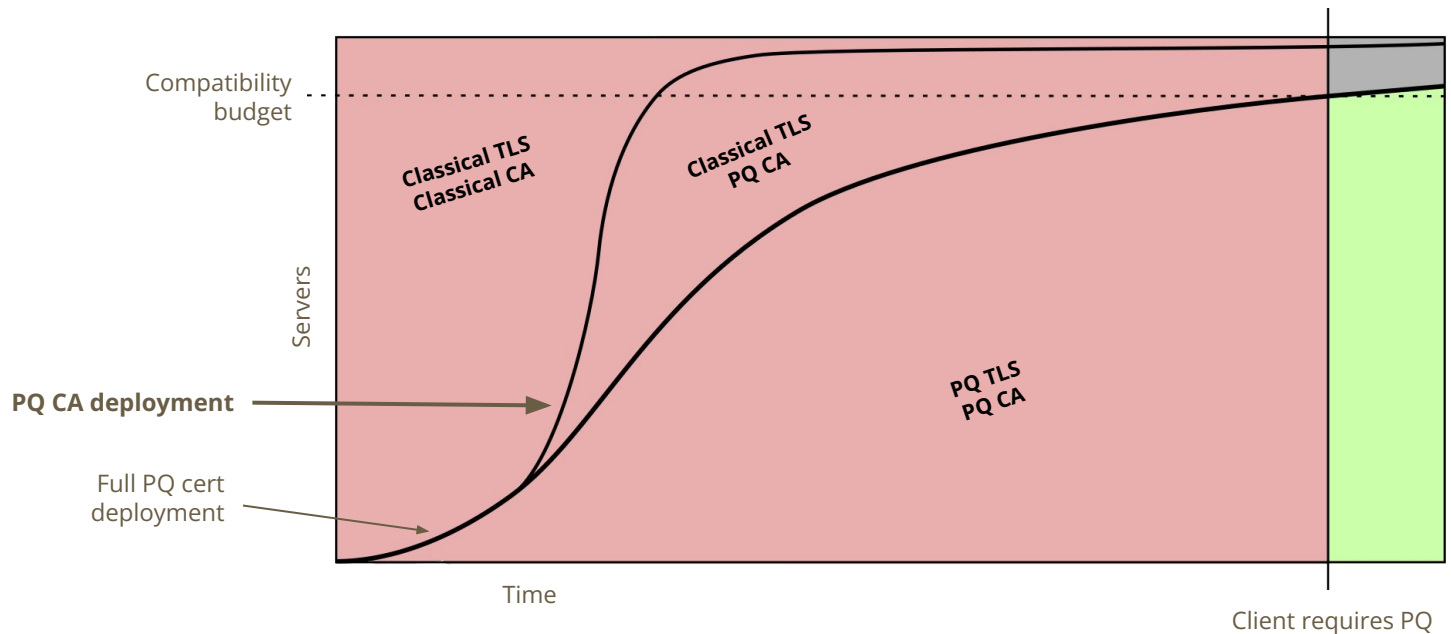
- Update software
- Maintain both traditional and PQ TLS keys

Can CA key be switched with **per-CA** work?

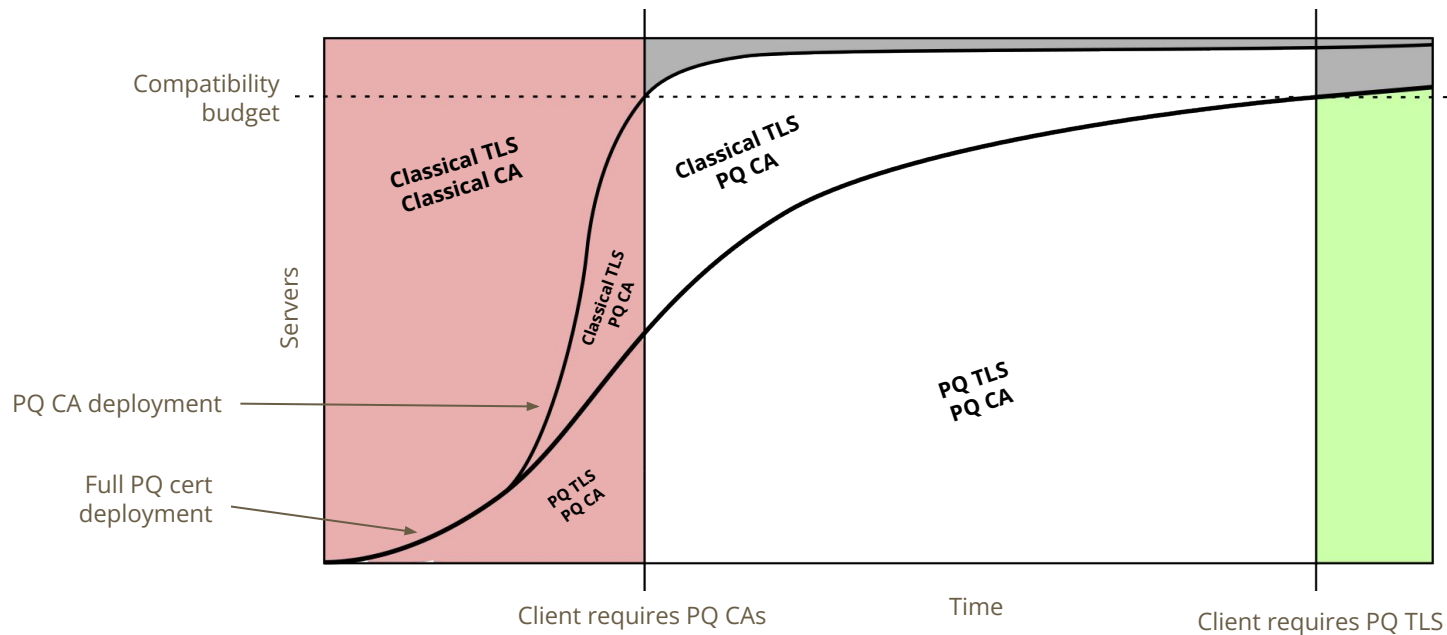
- Servers *already* renew certificates
- What if we automatically gave them certificates signed by the new CAs?



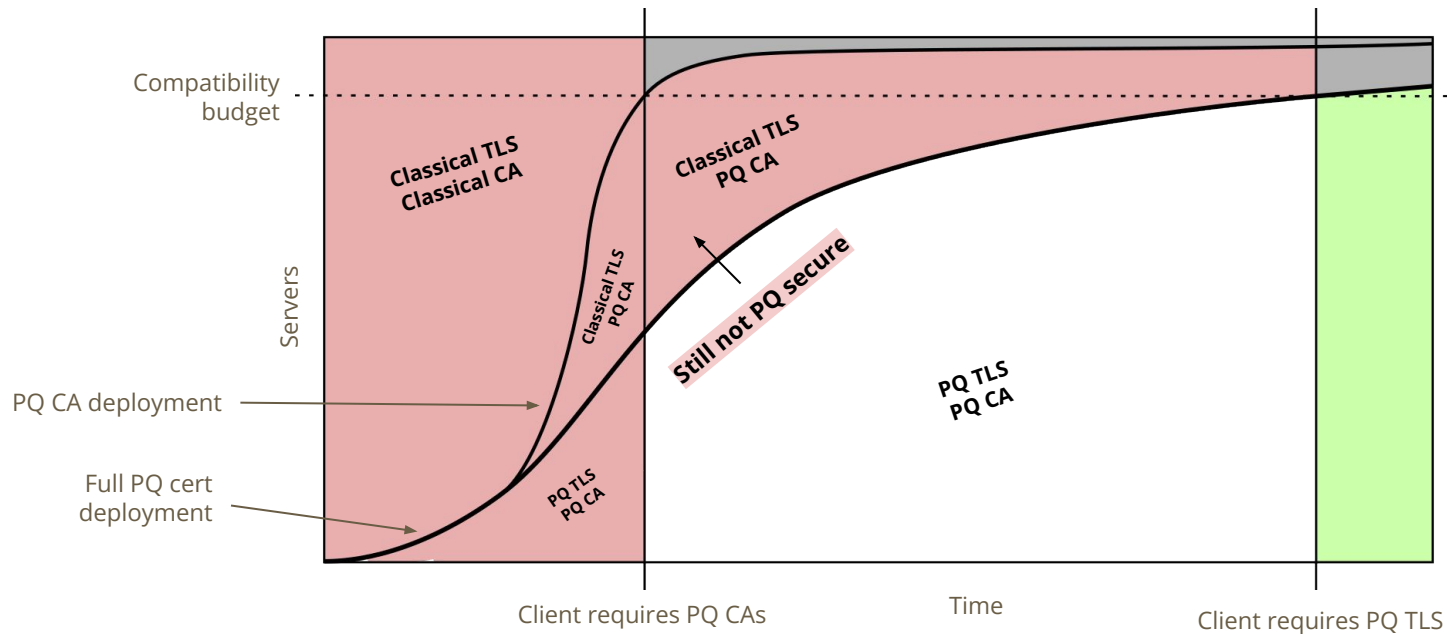
If we can automatically move to PQ CAs...



...the client can *require* PQ CAs sooner



Classical TLS keys are still weak



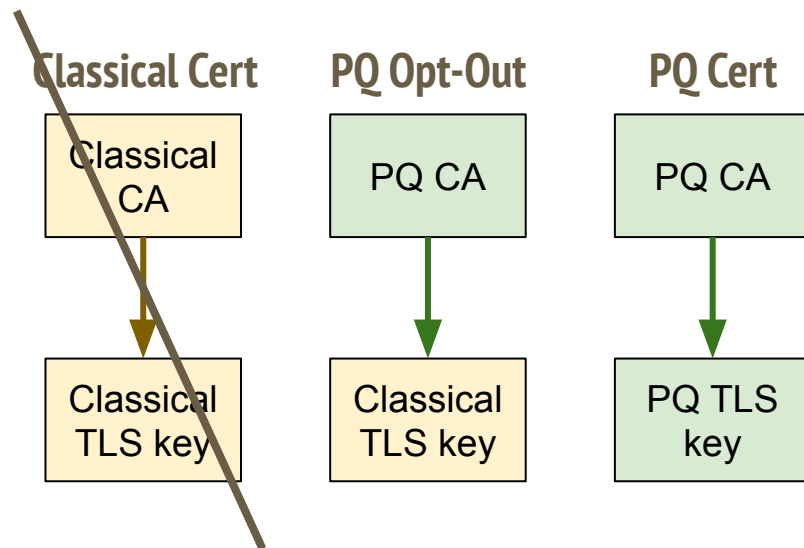
What is this transition state?

This is a **post-quantum opt-out certificate**

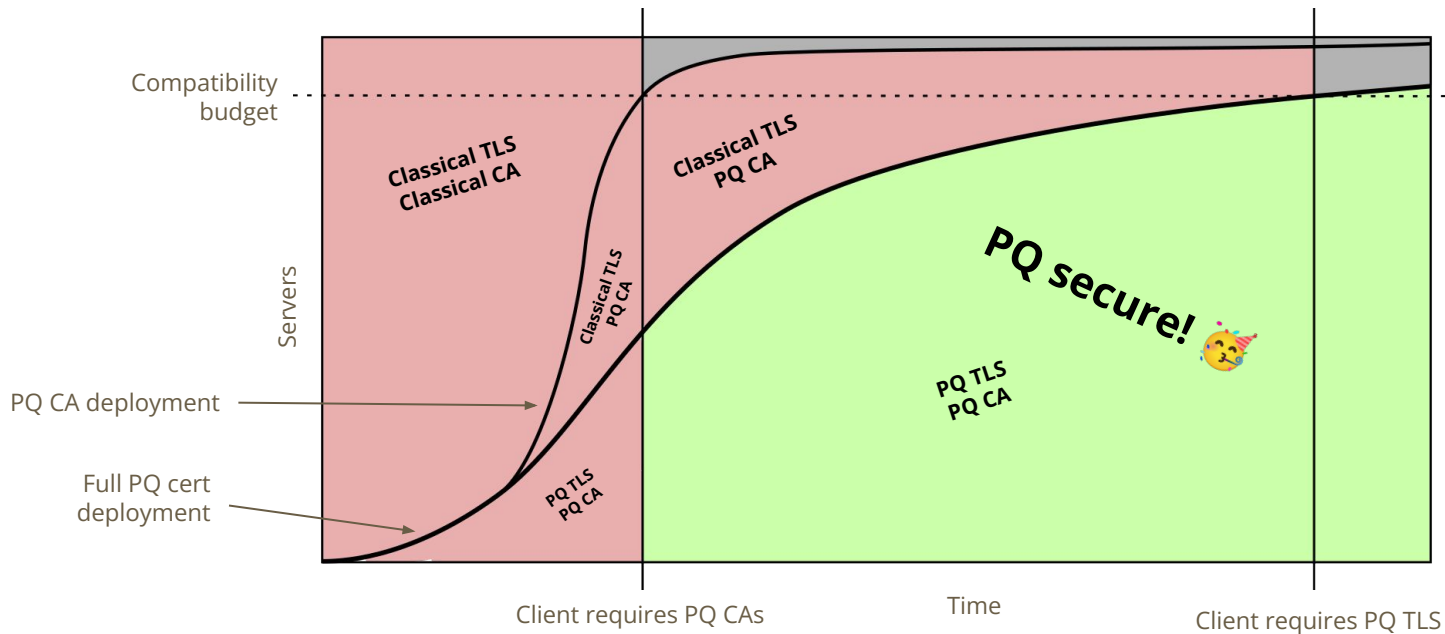
It is a *PQ-secure signal* that *this service is not yet ready for PQ*

Clients can drop classical CAs and *remain compatible with opt-out certificates*

Without classical CAs, **attackers cannot make clients think a PQ-secure server has opted out**



PQ TLS is no longer vulnerable to classical CAs



Making opt-out certificates work

What did I sweep under the rug?

But servers have to talk to old clients...

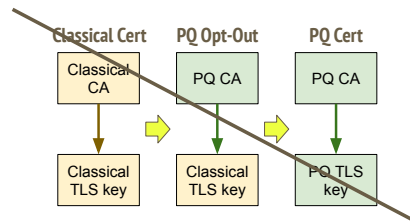
Servers have their own S-curve problem

- Switching to a PQ CA breaks old clients
- Keeping a classical CA holds back new clients

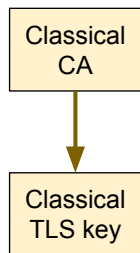
If it's not safe for the server, the CA cannot do it automatically

Deploy multiple certificates

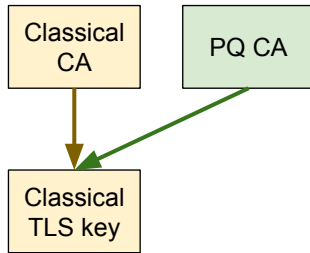
Select the right certificate for each client



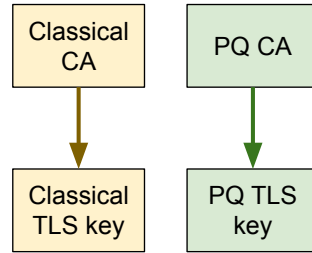
Today's Servers



PQ Opt-Out Servers



PQ Servers

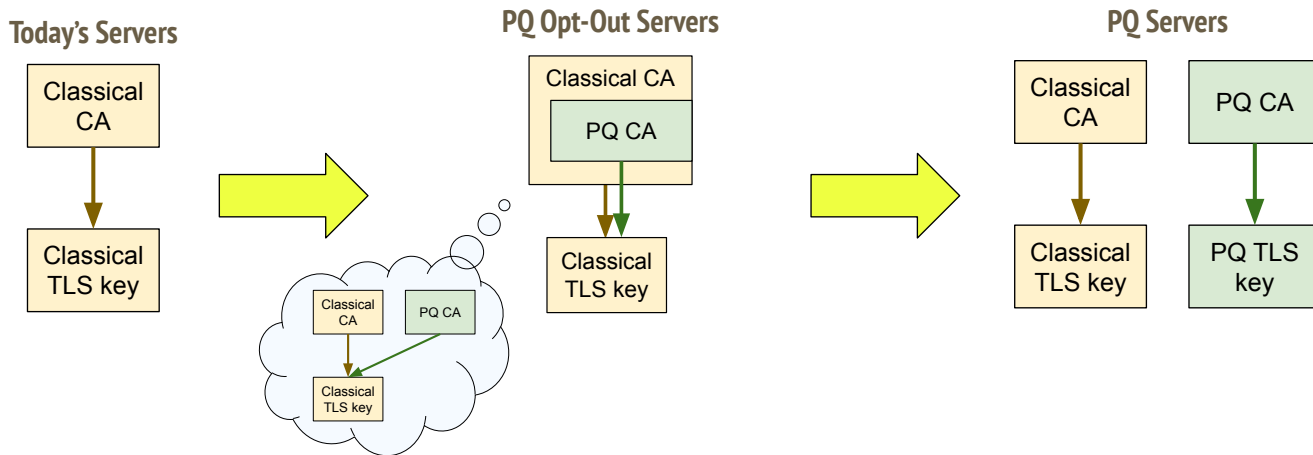


Legacy servers cannot configure two certificates

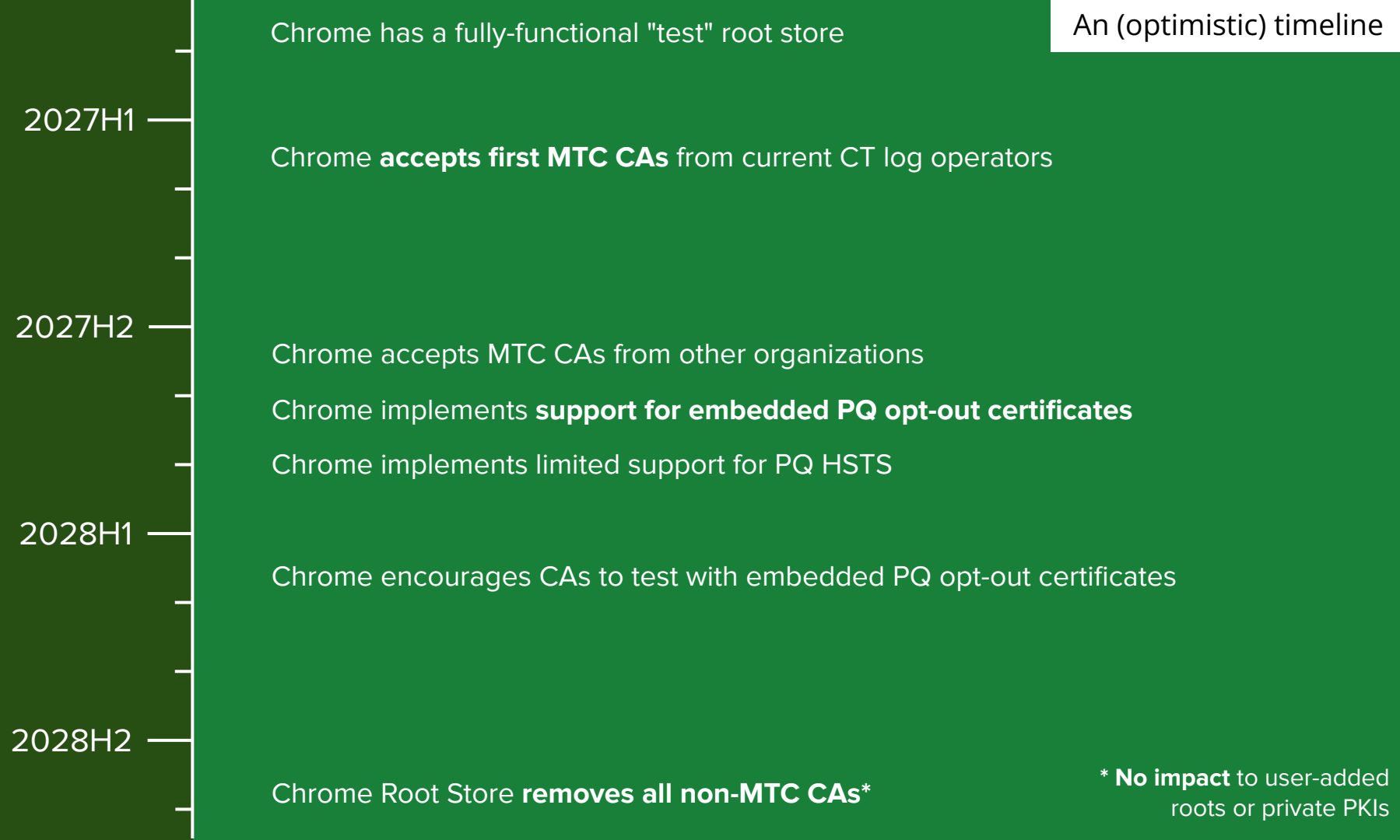
Many of today's legacy servers can only handle one certificate

Follow Alex's guidebook and... jam one certificate inside the other 🥹

One-time transitional hack — post-transition, servers assumed multi-certificate-capable

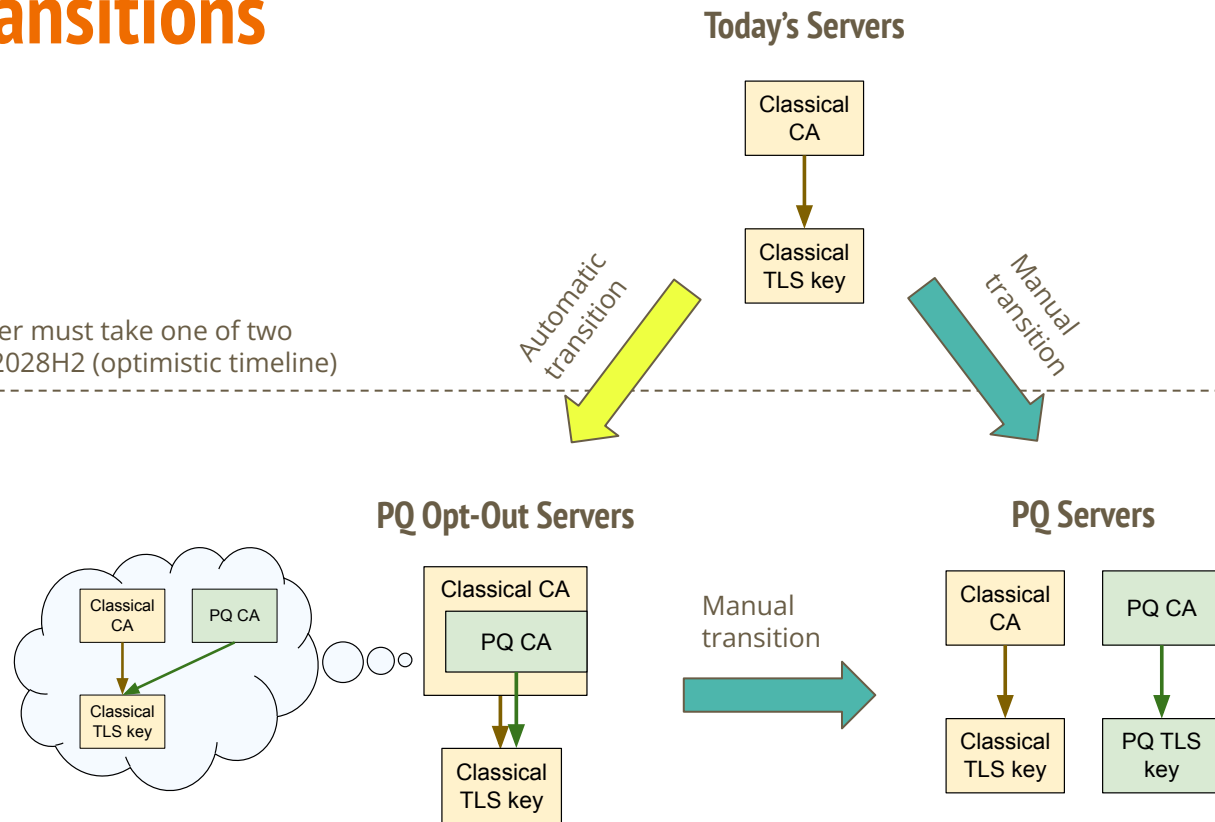


An (optimistic) timeline



Server transitions

Every server must take one of two paths by 2028H2 (optimistic timeline)



Opt-out servers should still move to post-quantum *eventually*

Post-quantum transition takeaways

Adding post-quantum trust anchors is not enough

To protect servers, **clients must remove all classical CAs**

If you trust **even one classical CA**, you have no post-quantum security

Legacy clients and legacy servers **will last for many years** and must keep working during the transition

We need a backwards-compatible, automatic **post-quantum opt-out** construction for legacy servers

It is not only safe but **useful** for PQ CAs to sign classical end-entity keys