

The road ahead to a fully post-quantum Internet



Bas Westerbaan, Cloudflare Research
BE-CYBER 2026, Sep 22nd, Wavre

About Cloudflare

We run a **global network** spanning 335 cities in over 125 countries.

Started of as a **CDN** and **DDoS mitigation** company, we now offer many more services, including

- **1.1.1.1**, public DNS resolver
- **Workers**, developer platform
- **Zero trust**, to protect corporate networks

We serve **20%+ of all websites** and process 115 million HTTP requests per second.
>45% of Fortune 500 are paying customers.



Helping build a better Internet

Cloudflare cares deeply about a **private**, **secure** and **fast** Internet, helping design, and adopt, among others:

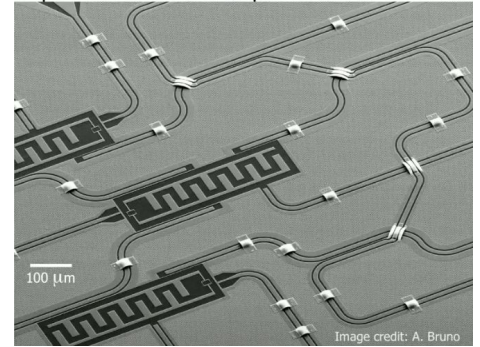
- Free TLS certificates (2014), TLS 1.3 and QUIC
- Encrypted DNS
- Private Relay / OHTTP
- Encrypted ClientHello

And, you will not be surprised:

- Migrating the web to post-quantum cryptography.



Quantum computers are great: **efficient simulation of nature** → new materials & medicine!



Minor inconvenience: they'll **break much of cryptography.**

(AES-128 and SHA-256 are not threatened.)

Solution: migrate to post-quantum cryptography (PQC).

When is it **expected** quantum computers
break RSA-2048?

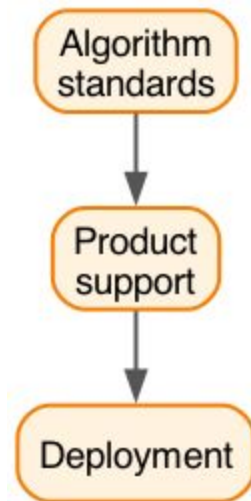
(I think before 2035.)

When is it ~~expected~~ quantum computers
break RSA-2048?

When is it possible quantum computers break RSA-2048?

We think 2030, so are migrating by [2029](#).

Ok, let's migrate to PQC! What's the steps?



ML-KEM and ML-DSA
were standardized August
2024—we can add
support to products!

An algorithm is not enough: we also need standards on how to integrate it into higher-level protocols and systems.

Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3

RFC 10024

Status

Email exp

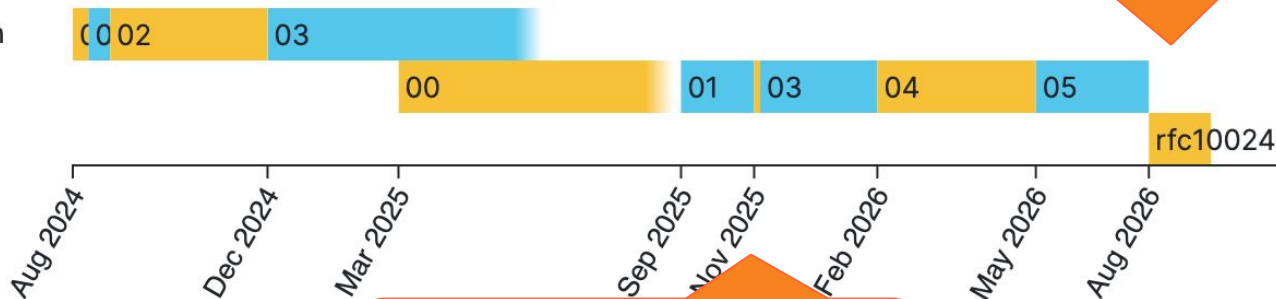
ML-KEM
standardized.

Official
standard

draft-kwiatkowski-tls-ecdhe-mlkem

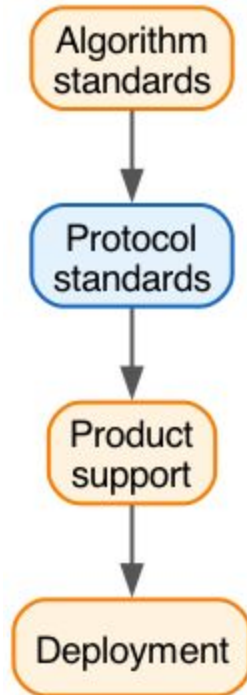
draft-ietf-tls-ecdhe-mlkem

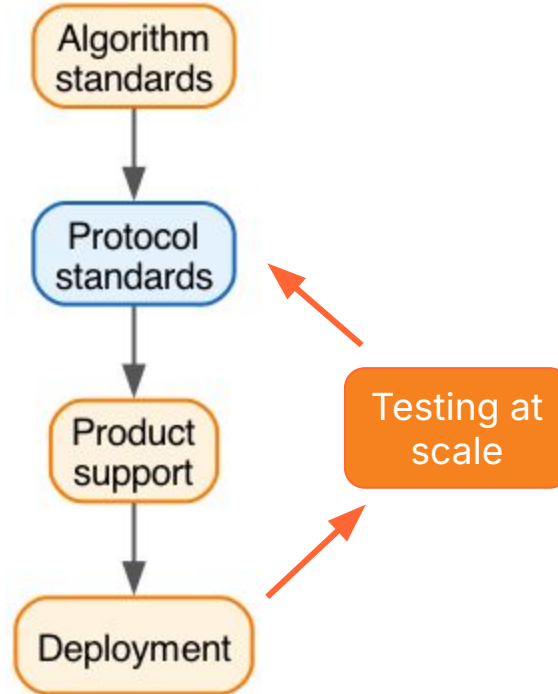
rfc10024



Early testing
in 2022

50% of browsers
use ML-KEM





Most systems can't upgrade all at once.

Protocol agility in theory



Alice	Bob	Safe?
Vulnerable	Vulnerable	No
PQ supported Alice: my job is done, just waiting for Bob!	Vulnerable	No
PQ supported	PQ supported Bob: all good!	Yes

First gap: no common algorithm



Alice	Bob	Safe?
Vulnerable	Vulnerable	No
PQ-A supported Alice: my job is done, just waiting for Bob!	Vulnerable	No
PQ-A supported	PQ-B supported Bob: my job is done, just waiting for Alice!	No!

Which algorithm? (TLS certificates)

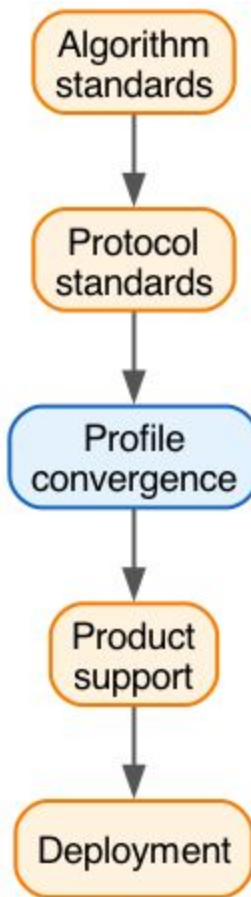
- MLDSA44-RSA2048-PSS
- MLDSA44-RSA2048-PKCS15
- MLDSA44-Ed25519
- MLDSA44-ECDSA-P256
- MLDSA65-RSA3072-PSS
- MLDSA65-RSA3072-PKCS15
- MLDSA65-RSA4096-PSS
- MLDSA65-RSA4096-PKCS15
- MLDSA65-ECDSA-P256
- MLDSA65-ECDSA-P384
- MLDSA65-ECDSA-brainpoolP256r1
- MLDSA65-Ed25519
- MLDSA87-ECDSA-P384
- MLDSA87-ECDSA-brainpoolP384r1
- MLDSA87-Ed448
- MLDSA87-RSA3072-PSS
- MLDSA87-RSA4096-PSS
- MLDSA87-ECDSA-P521
- MLDSA44
- MLDSA65
- MLDSA87
- slh-dsa-sha2-128s
- slh-dsa-sha2-128f
- slh-dsa-sha2-192s
- slh-dsa-sha2-192f
- slh-dsa-sha2-256s
- slh-dsa-sha2-256f
- slh-dsa-shake-128s
- slh-dsa-shake-128f
- slh-dsa-shake-192s
- slh-dsa-shake-192f
- slh-dsa-shake-256s
- slh-dsa-shake-256f
- hash-slh-dsa-sha2-128s
- hash-slh-dsa-sha2-128f
- hash-slh-dsa-sha2-192s
- hash-slh-dsa-sha2-192f
- hash-slh-dsa-sha2-256s
- hash-slh-dsa-sha2-256f
- hash-slh-dsa-shake-128s
- hash-slh-dsa-shake-128f
- hash-slh-dsa-shake-192s
- hash-slh-dsa-shake-192f
- hash-slh-dsa-shake-256s
- hash-slh-dsa-shake-256f

Which algorithm? (TLS certificates)

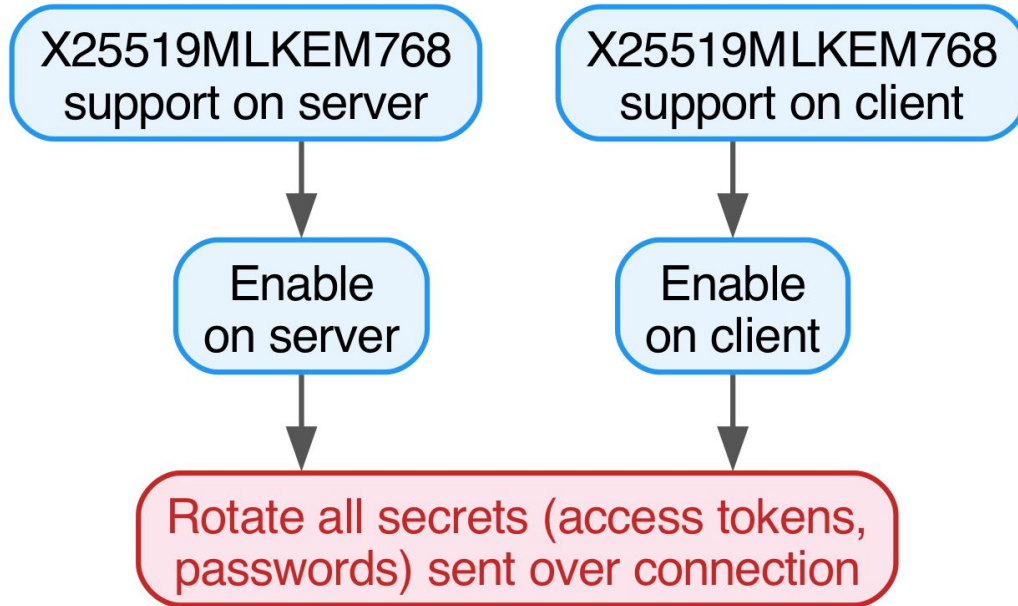
- MLDSA44-RSA2048-PSS
- MLDSA44-RSA2048-PKCS15
- MLDSA44-Ed25519
- MLDSA44-ECDSA-P256
- MLDSA65-RSA3072-PSS
- MLDSA65-RSA3072-PKCS15
- MLDSA65-RSA4096-PSS
- MLDSA65-RSA4096-PKCS15
- MLDSA65-ECDSA-P256
- MLDSA65-ECDSA-P384
- MLDSA65-ECDSA-brainpoolP256r1
- MLDSA65-Ed25519
- MLDSA87-ECDSA-P384
- MLDSA87-ECDSA-brainpoolP384r1
- MLDSA87-Ed448
- MLDSA87-RSA3072-PSS
- MLDSA87-RSA4096-PSS
- MLDSA87-ECDSA-P256
- MLDSA44
- MLDSA65
- MLDSA87

Reading the tea
leaves, MLDSA44
will have broad
support

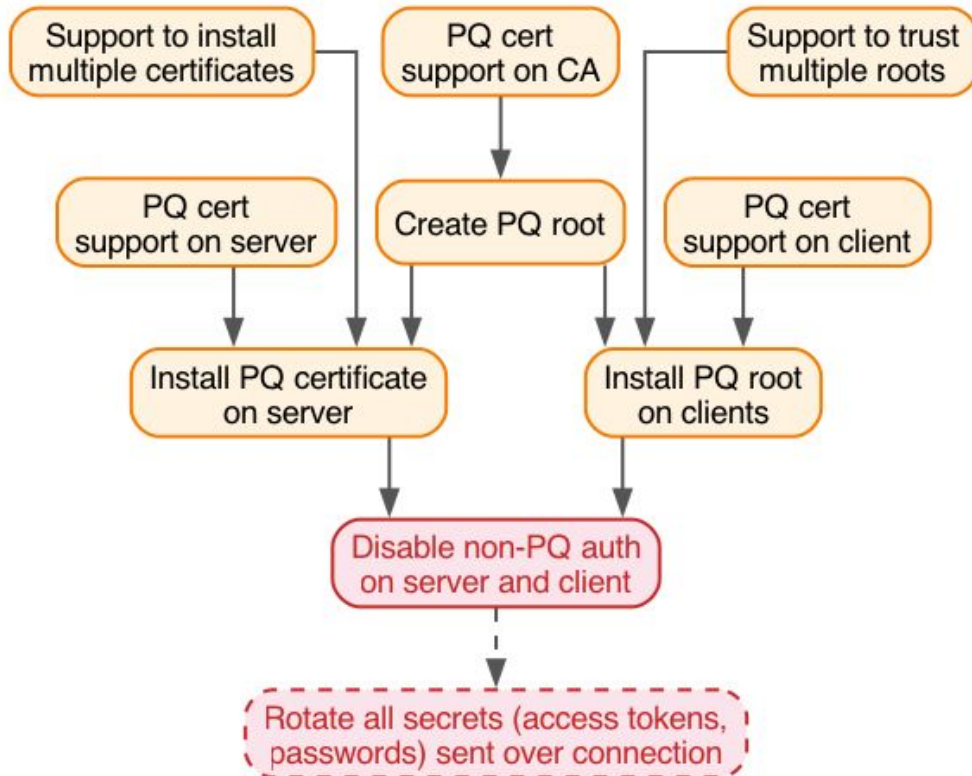
- slh-dsa-sha2-128s
- slh-dsa-sha2-128f
- slh-dsa-sha2-192s
- slh-dsa-sha2-192f
- slh-dsa-sha2-256s
- slh-dsa-sha2-256f
- slh-dsa-shake-128s
- slh-dsa-shake-128f
- slh-dsa-shake-192s
- slh-dsa-shake-192f
- slh-dsa-shake-256s
- slh-dsa-shake-256f
- hash-slh-dsa-sha2-128s
- hash-slh-dsa-sha2-128f
- hash-slh-dsa-sha2-192s
- hash-slh-dsa-sha2-192f
- hash-slh-dsa-sha2-256s
- hash-slh-dsa-sha2-256f
- hash-slh-dsa-shake-128s
- hash-slh-dsa-shake-128f
- hash-slh-dsa-shake-192s
- hash-slh-dsa-shake-192f
- hash-slh-dsa-shake-256s
- hash-slh-dsa-shake-256f

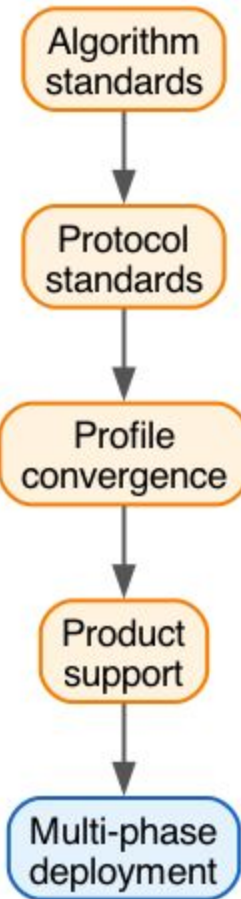


Mitigating HN/DL for TLS is “easy”



Post-quantum certs in TLS has more steps





Protocol agility in theory

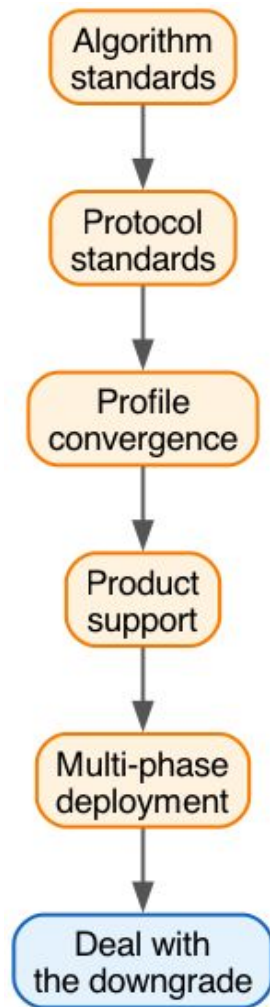


Alice	Bob	Safe?
Vulnerable	Vulnerable	No
PQ supported Alice: my job is done, just waiting for Bob!	Vulnerable	No
PQ supported	PQ supported Bob: all good!	Yes

Second gap: downgrades

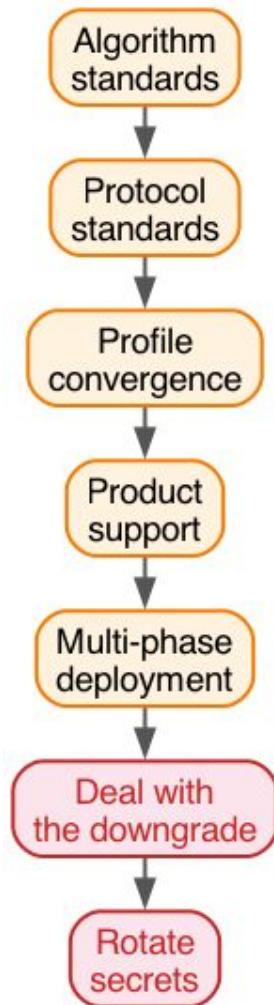


Alice	Bob	Safe?
Vulnerable	Vulnerable	No
PQ & vulnerable	Vulnerable	No
PQ & vulnerable	PQ & vulnerable	No!

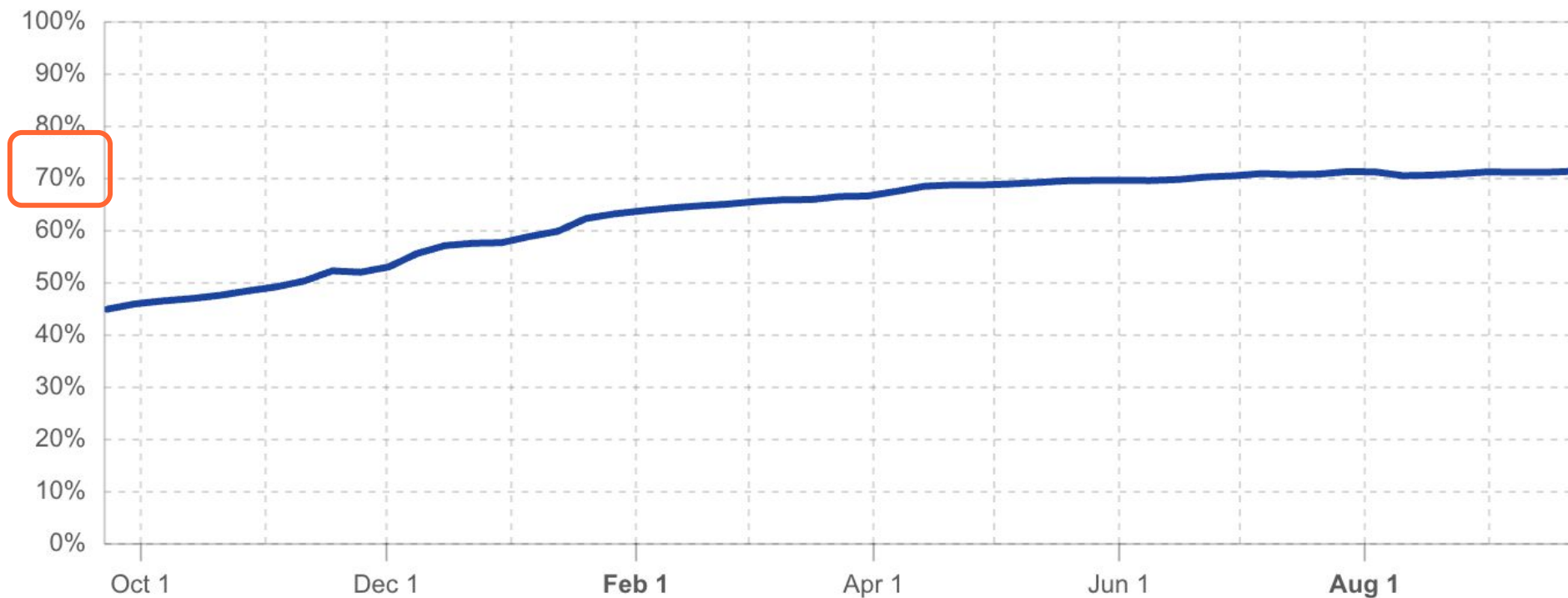


Turning off support for vulnerable cryptography on client and server prevents downgrades, but in most large systems this is simply impossible.

There are solutions, but they are protocol specific. [Current thinking for TLS.](#)

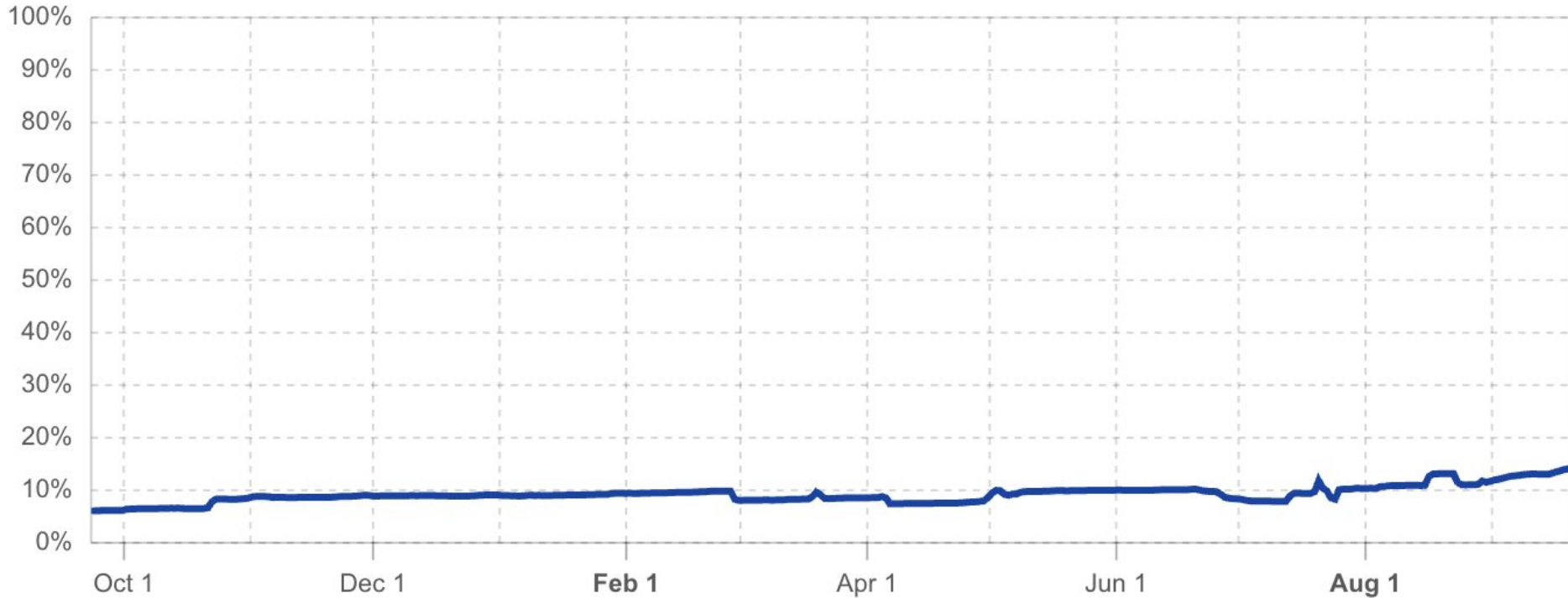


Cloudflare visitor support for x25519MLKEM768



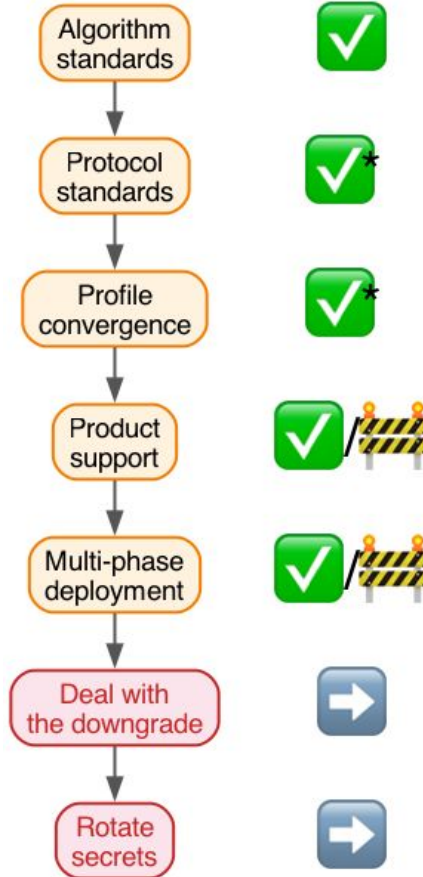
September 2025–2026 from radar.cloudflare.com/post-quantum

Support at Cloudflare customer's origins



September 2025–2026 from radar.cloudflare.com/post-quantum

HNDL



Post-quantum certificate deployment in the WebPKI?

(nothing)

... but widespread deployment coming early 2027.

We're in the experimental phase now.

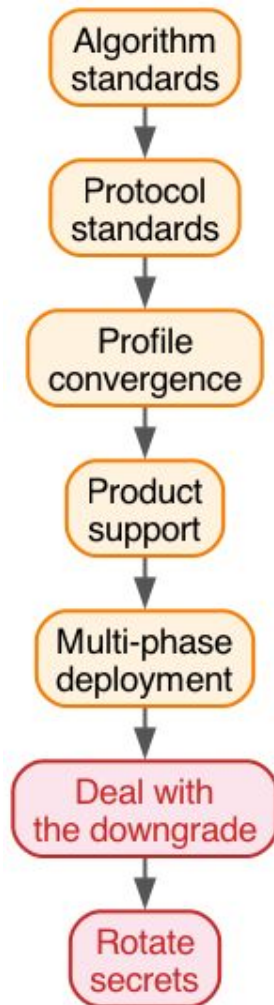


	HNDL	Certs	CT	ECH
Algorithm standards	✓	✓	✓	?
Protocol standards	✓*	✓/🚧	🚧	✗
Profile convergence	✓*	✓/🚧	🚧	✗
Product support	✓/🚧	🌱	🧪	✗
Multi-phase deployment	✓/🚧	📅 17	📅 17	✗
Deal with the downgrade	➡	➡	🌱	
Rotate secrets	➡	✗		

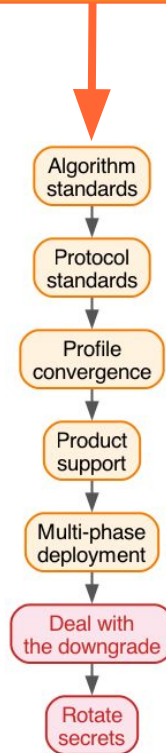
	HNDL	Certs	CT	ECH	DNSSEC
Algorithm standards	✓	✓	✓	?	?
Protocol standards	✓*	✓/🚧	🚧	✗	🔬
Profile convergence	✓*	✓/🚧	🚧	✗	✗
Product support	✓/🚧	🌱	🧪	✗	✗
Multi-phase deployment	✓/🚧	📅 JUL 17	📅 JUL 17	✗	✗
Deal with the downgrade	➡	➡	🌱		✗
Rotate secrets	➡	✗			

This is *just* the browser / website ecosystem.

The post-quantum migration is a **marathon** that every ecosystem runs at their **own pace**.



Awareness / sense of urgency



What should organizations do now?

Deploy where available—or even just a **pilot**.

Best practices help: keep software up-to-date, use modern protocols, automated rotation of secrets and issuance.

But first and foremost:

- Determine the **business continuity impact** of a quantum emergency. This is not a CBOM.
- Think of (non-cryptographic) mitigations.
- Prepare a **quantum emergency recovery playbook**.

In summary

- We have the NIST standards. They'll have to do.
- Agility: you surface technical gaps by trying.
- The more federated an ecosystem is, the more important it is to pick a small set of common algorithms.
- You're not done until you've dealt with downgrades!
- We need recovery playbooks, not inventories.

Thank you, questions?

blog.cloudflare.com/post-quantum-roadmap