Post-quantum beyond TLS: what Cloudflare's Privacy Pass post tells us about planning

10 November 2026 · 5 min read · blogs.iictp.org/post-quantum-privacy-pass-q-day-planning

Most post-quantum discussion is about TLS, the protocol that secures connections. Cloudflare's 6 November post looks at something less visible: Privacy Pass, a protocol that lets sites limit abuse without identifying users.

TL;DR The short version

- Cloudflare's 6 November post looks at post-quantum cryptography beyond TLS, using Privacy Pass, which limits abuse without identifying users.
- It says key agreement comes first, but much more than TLS relies on quantum-vulnerable cryptography.
- Teams can start without being cryptographers by listing every place they rely on public-key cryptography.

Read online, listen to it, or change the text size: https://blogs.iictp.org/post-quantum-privacy-pass-q-day-planning

What the post says

- Cloudflare says the first priority for the post-quantum transition is the building blocks of authenticated key-agreement protocols such as TLS, since secure communication will not be possible without them once cryptographically relevant quantum computers exist.
- It also says we rely on quantum-vulnerable cryptography for much more than TLS, and Privacy Pass is one example: it still uses classical cryptography such as RSA and elliptic curves.
- Per Cloudflare, a quantum attacker could forge tokens and bypass controls such as rate limiting, but Privacy Pass is unconditionally private, so a quantum attacker still could not link a token's redemption to its issuance.
- Cloudflare describes post-quantum alternatives as an active research area and says the new capabilities it is developing can keep the same privacy guarantee after "Q-day".

A planning exercise for your team

You do not need to be a cryptographer to act on this. You need an inventory.

- List every place your systems use public-key cryptography: TLS, code signing, tokens, VPNs, device identity, document signing, backups.
- For each, note whether a break would let an attacker read old data, forge new data, or both. They need different timelines.
- Note which vendors and libraries own each one, and ask when they plan to support post-quantum options.
- Make cryptography replaceable in new designs: avoid hard-coding algorithms in places that are hard to change.

Facts in this post were read from the sources listed below on 10 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. Cloudflare Blog. The post-quantum future of web privacy. 6 November 2026. blog.cloudflare.com/vole-mole/

Published by IICTP, an independent technical credential body, on 10 November 2026. The current version of this post is at https://blogs.iictp.org/post-quantum-privacy-pass-q-day-planning. More guides: blogs.iictp.org.