https://datatracker.ietf.org/doc/draft-farrell-tls-pqg/

IETF 124, October 2025

stephen.farrell@cs.tcd.ie

Guidance for current PQ deployments

- Start using hybrid KEMs, e.g. (or especially?) equivalents to X25519MLKEM768, whenever you can
  - Once you can do that, don’t fallback to ECDH or “pure’’ PQ except when you have to
- For almost everyone, do nothing abut signatures now
  - TODO: define “almost everyone” better
- To be useful: this needs to be extremely terse (IMO)

Why?

- We have a plethora of WGs defining a plethora of PQ things so we should tell people to not take all those as equally ready for deployment now
  - draft-ietf-lamps-pq-composite-sig defines 18 alg-ids and there are load of other LAMPS PQ drafts
  - OpenPGP PQ stuff adds 17 (in a 1-octet space)
  - Other WGs doing similar: TLS, SSHM, HPKE, MLS, IPSECME, JOSE, COSE and CFRG (and maybe KITTEN too soon)
  - We seem to be keen to define almost all possible PQ options for everything
- I don’t like all of the above but it seems unstoppable, so we should provide some guidance to save people from wasting lots of time and maybe making interop or security worse by deploying things that are not ready

Where?

- Some people will prefer /dev/null
- Could fit into PQUIP except I’ve not seen PQUIP as being willing to be skeptical
- Could be OPSAWG
- Could be AD sponsored