TLS Registries Update (Since IETF 119)

Rich Salz, Sabrina Tanamal

Changes

- ALPN: Added Postgresql
- Nothing but post-quantum
- Khyber/25519 and Khyber/p256 marked obsolete
- New single draft for all hybrids of {P256r1, P384r1, X25519} with ML-KEM 768
  - Much bikeshedding
  - .. and how do you feel about FIPS? :)
- Added ML-KEM 512 768 1024
  - But no reserving specific magic numbers (again)