-rfc8446bis

IETF 120 - TLS WG
Sean Turner (channeling ekr)

Datatracker: draft-ietf-tls-rfc8446bis
GitHub: tls13-spec

Status / Queued PRs

Status:

- Merged #1351 & #1353: errata 6820 & 8442
- Merged #1361: Unify client and server certificate selection text
- Merged #1354: Forbid the sender from sending duplicate supported groups entries

Queued PRs:

- #1357 addresses errata: 6151, 6152, 7003, 7073, & 7620 (thanks Ben Smyth)
  - Do small tweak, then merge.
- #1360 makes x25519 an MTI (see next slide)

PSA: Keep it Professional!

Add x25519 as an MTI (aka MUST support)?

PR:

> A TLS-compliant application MUST support key exchange with secp256r1 (NIST P-256) and ~~SHOULD support key exchange with~~ X25519 {{RFC7748}}.

BUT, 1st we have to decide whether to even entertain this PR; see next slide.

Hums

Hum 1: Is it appropriate to make this change in this I-D, which was supposed to be just for clarifications. y/n

Hum 2 IFF Hum 1 is y:

Support making this change or not? y/n