TLS Registries Update

Rich Salz*, Sabrina Tanamal (IANA)

IETF 119

Miscellany

- Experts: Yoav Nir, Rich Salz, Nick Sullivan; two of three needed

- Still zero rejections

- Upcoming: protocols and algorithms will require TLS WG agreement or consensus or *something*
  - Intent is ALPN, exporters, etc., do not.

Extensions

- ~~In progress: Hybrid X509 from ASC X9.146 (ANSI, ISO to follow); allows client and server to pick which key in a hybrid cert to use, or both~~
  Withdrawn; it was premature

- DTLS return_routability_check:
  - `61   rrc   CH, SH   Y   N    [draft-ietf-tls-dtls-rrc-10]`

- ECH: encrypted_client_hello, ech_outer_extensions, ech_required (temporary alert)

Cipher Suites, Signatures, Groups

- Nothing new

ALPN and Exporters

- One in-progress:
  - "co" CoAP (over DTLS)
  - "coap" text changed to "CoAP (over TLS)"

- No new exporters