Updates for PCEPS: TLS Connection Establishment Restrictions

IETF 118 - PCE WG

Dhruv Dhody, **Sean Turner**, & Russ Housley

Datatracker: draft-ietf-pce-pceps-tls13
GitHub: kyber-certificates

Status

WGLC on -01 ended on 20 September 2023

Comments from Shephard (Andrew Stone), Stephane Litkowski, & Cheng Li

- Multiple Commenters:
  - Make title more explicit: Updates for PCEPS*: TLS Connection Establishment Restrictions*
  - Make RFC 8253 Security Considerations explicitly part of this I-D
- Stephane's resulted in "big" changes:
  - Q: What's different than what's already in RFC 8253.
  - A: Not much:
    - Updates "TLS Connection Establishment Restrictions" (Section 3.4) of RFC 8253 <- new title
    - Add restrictions to specify what PCEPS implementations do if a PCEPS supports more than one version of the TLS protocol and to restrict the use of TLS 1.3's early data.
    - Dropped algorithm requirements as already covered in RFC 8253.