PCEPS with TLS 1.3

draft-dhody-pce-pceps-tls13-01

Dhruv Dhody, Sean Turner, Russ Housley

Motivation

- RFC 8253 defines how to protect PCEP messages with TLS 1.2.
- This document defines how to protect PCEP messages with TLS 1.3.
  - Be explicit about TLS 1.3 profile
  - Address 0-RTT (Early-Data) and cipher suites
  - All else is based on RFC 8253
- Similar work adopted in the NETCONF WG.

0-RTT (Early Data)

- 0-RTT/Early data in TLS 1.3 allows a client to send data as part of the first flight of messages to a server.
- TLS 1.3 can be used without early data.
  - In fact, early data is permitted by TLS 1.3 only when the client and server share a Pre-Shared Key (PSK), either obtained externally or via a previous handshake. The client uses the PSK to authenticate the server and to encrypt the early data.
- The security properties for early data are weaker than those for subsequent TLS-protected data.
  - In the absence of an application specific profile, TLS 1.3 says MUST NOT use 0-RTT.
  - This document explicitly says that PCEPS implementations that support TLS 1.3 **MUST NOT** use early data.

Cipher Suites

- Algorithms are different than those in TLS 1.2.
- The mandatory-to-implement algorithms are forward secure.

PCEP-YANG & TLS1.3

Update to PCEP-YANG

- The YANG module uses the TLS grouping in [I-D.ietf-netconf-tls-client-server] which support TLS 1.2 and 1.3.
- Note that any TLS version can be configured via [I-D.ietf-netconf-tls-client-server] but it recommends TLS 1.3.
- TLS 1.2 is still in use for PCEP and can be enabled with feature "tls12".
  - even though it is marked with status as "deprecated"!
- This description has been added in the draft.

THANKS!

Lets adopt this work?