Working Group Draft for TCPCLv4

Brian Sipos

RKF Engineering Solutions

IETF108

Motivations for Updates to TCPCL

1. During implementation of TCPCLv3, Scott Burleigh found an ambiguity in bundle acknowledgment and refusal.
2. For use in a terrestrial WAN, author has a need for TLS-based authentication and integrity. TCPCLv3 mentions TLS but does not specify its use. IETF strongly in favor of TLS for new general-use protocols.
3. Reduced sequencing variability from TCPCLv3
4. Adding extension capability for TCPCL sessions and transfers.

Goals for TCPCLv4

- Do not change scope or workflow of TCPCL.
  - As much as possible, keep existing requirements and behaviors. The baseline spec was a copy-paste of TCPCLv3.
  - Still using single-phase contact negotiation, re-using existing headers and message type codes.
  - Allow existing implementations to be adapted for TCPCLv4.
- Add long-term extensibility and interoperable security.

Latest Draft Changes

- Editorial changes based on IESG and AD feedback.
- Added Section 3 descriptive subsections for:
  - PKIX Environments and CA Policy – Explaining the rationale of supporting Node ID and DNS-ID certificate authentication.
  - Session Keeping Policies – Explaining the extremes of how a BP agent can use TCPCL sessions, including push vs. pull (polling).
- Made separate proposal for how a CA can validate ownership of a Node ID in draft-sipos-acme-dtnnodeid.
- No further comments have been received.
- Waiting for final IESG reviews.

Remaining Issues

- One behavioral issue brought up in IESG review is the coupling between CL peer authentication and Bundle Protocol Agent (BPA) verification:
  - The CL can authenticate that the peer has a Node ID authenticated by a trusted PKIX CA.
  - When the CL session changes state to *Established* the peer Node ID is available to the BPA.
  - There is the potential for a BPA to attempt a CL session with `dtn://nodeA/bpa` and actually gets a peer `dtn://nodeB/bpa`.
  - What requirements are on the BPA to ensure that the peer Node ID is the one desired? And what does a BPA do if the Node ID is not expected? Should the CL care?