Working Group Draft for TCPCLv4

BRIAN SIPOS

RKF ENGINEERING SOLUTIONS

IETF109

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 CL security.

Latest Draft Changes

Changes were made in `draft-ietf-dtn-tcpclv4-22`.

Editorial changes based on feedback from Benjamin Kaduk:

- Made peer authentication methods as SHALL and fixed ambiguity about how to handle failure vs. absent identifier. If a certificate contains a SAN identifier and it does not match, the handshake fails regardless of policy.
- Renamed term NETWORK-ID to IPADDR-ID and clarified “host name” to “DNS name”

Added clarification about receiving (and authenticating) a peer Node ID different than expected.

Received later feedback from Martin Duke. Changes were pending I-D submission freeze:

- Touched up TLS authentication description and requirements to simplify logic.
- Added XFER_REFUSE reason of “Session Terminating” to distinguish from other, data-related reasons.
- Confirmed other comments via mailing list.

Waiting for further IESG reviews.

Remaining Questions

How to define the use of CAN_TLS contact header flag?

- This is a question of phrasing and conditions more than technical capability.

Adding a "supported versions set" to the Contact Header is possible to make version negotiation easier?

- It would expand the CH and make it variable-sized.
- How likely are entities to run multiple TCPCL versions?

Is there a need for a DTN-specific Extended Key Usage OID?

- Without this, I can re-purpose my HTTPS certificate and use it for TCPCL (DNS name) authentication if the peer policy allows DNS-ID-only certificates. Is that desirable?