ACME DTN Node ID Validation

BRIAN SIPOS

RKF ENGINEERING SOLUTIONS

IETF108

DTN Background

- DTN Architecture in RFC 4838
- Store-and-forward of Bundles
  - Similar to email over SMTP
- Overlay network
  - Rely on Convergence Layer adaptors for bundle transport between nodes
  - Late binding of Endpoint IDs
  - Bundle forwarding and routing
- End-to-end and per-hop security mechanisms

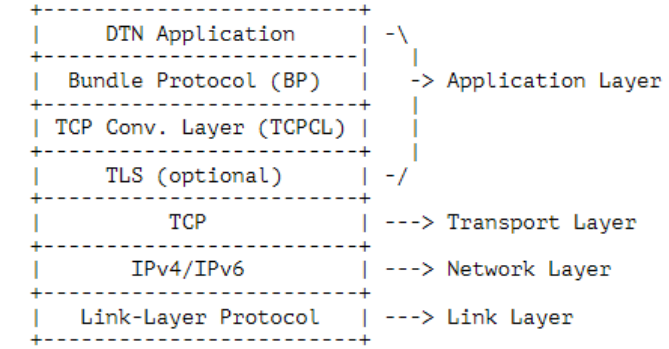
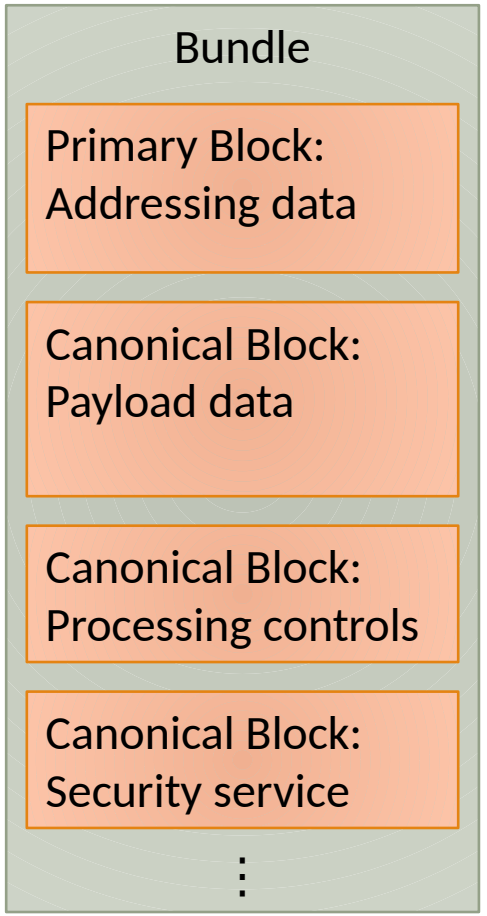


Figure 1: The Locations of the Bundle Protocol and the TCP Convergence-Layer Protocol above the Internet Protocol Stack

DTN Bundles

- The Bundle is the protocol data unit of DTN BP.
- A Bundle is composed of blocks.
  - One Primary block with addressing and bundle-wide parameters.
  - Sequence of Canonical blocks with type-code and block-type-specific-data.
- One canonical block is the Payload.
  - Administrative Record payloads are addressed to Node ID and processed by BP agent.
- Each bundle is stand-alone unit.
  - Addressed to an Endpoint ID
  - Sourced by a Node ID
  - Source of admin. Records can be replied-to.
- Bundle Security (BPSec) can be used to cryptographically sign, MAC, or encrypt blocks.



Motivations for Node ID Validation

- Proposed DTN TCP Convergence Layer Version 4 defines a PKIX certificate authentication mechanism.
  - Two modes of authentication: Node ID (as URI) and DNS name.
  - DNS name validation defined in RFC 6125.
  - URI validation is defined by TCPCL (RFC 6125 has only DNS-related definition).
- Question was raised “How should a CA validate a DTN claim?”
- ACME provides a well-established mechanism to do all the important bookkeeping needed by a CA.
  - Prefer this over ad-hoc mechanisms that don’t provide strong guarantees of fitness.

Proposed Validation Mechanism

- Very similar to proposed [draft-ietf-acme-email-smime].
  - New BP Administrative Record type defined.
  - Challenge Bundle supplies token-part1.
  - ACME server supplies token-part2.
  - Response Bundle combines token and generates Key Authorization result.
- Recommends Bundle Integrity cryptographic signing.
  - Useful to pass network security policy.
  - Not needed for validation itself.

Desired WG Direction

- Currently drafted as Experimental.
  - The DTN protocols are entering Standards Track status.
  - No other ACME mechanisms currently validate URI claims.
- Proposed as “If you want to do this thing, here is the best way to achieve it.”
- Any desire by ACME WG to adopt a URI validation?
- Distinction between mandatory-to-implement and optional validation mechanisms?