ACME DTN Node ID Validation

BRIAN SIPOS

RKF ENGINEERING SOLUTIONS

IETF110

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
- Both end-to-end and per-hop security mechanisms are defined.

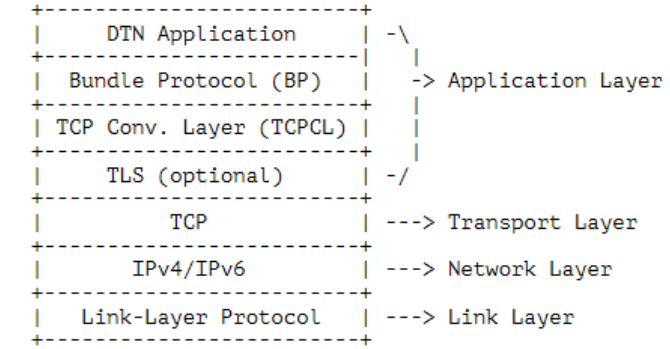

Figure 1: The Locations of the Bundle Protocol and the TCP Convergence-Layer Protocol above the Internet Protocol Stack

Motivations for Node ID Validation

- Proposed DTN Convergence Layers and Bundle Security 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

- Identical flow to [draft-ietf-acme-email-smime].
  - New BP Administrative Record type defined.
  - Challenge Bundle supplies token-part1.
  - ACME server, via HTTPS, supplies token-part2.
  - Response Bundle combines token and generates Key Authorization result, includes token-part1 to correlate.
  - ACME server compares response digest with expected.
- Recommends Bundle Integrity cryptographic signing.
  - Useful to pass network security policy.
  - Not needed for validation itself.

Draft Next Steps

- Currently drafted as Experimental.
  - The DTN documents are in RFC Editor Queue, as is ACME email validation.
  - 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.” Not expecting wide implementation in ACME.