JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

ACME DTN Node ID Validation

IETF 113 ACME WG

Brian Sipos
JHU/APL

Current Status of Draft

- Latest is https://www.ietf.org/archive/id/draft-ietf-acme-dtnnodeid-09.html
- Referenced DTN documents are now published RFCs!
- Changes since -06:
  - Added more detailed explanation of DTN terminology to explain what this validation covers (Administrative Endpoint ID) and what it does not (other types of Endpoint ID).
  - Separated “id-chal” “token-chal” and “token-bundle” to avoid overlaps in purpose and to behave more like RFC 8823 (email validation).
  - Added digest algorithm agility based on COSE example encoding.
    - SHA-256 is still mandatory-to-implement for interoperability.
  - Fixed typo in Section 3.1 “MUST NOT” changed to “MUST”.
  - Removed old identifier name “uri” and replaced with correct “bundleEID”.
  - Example bundles now use indefinite-length array framing.
- Known issues remaining:
  - The COSE Hash Algorithms document is still in AUTH48 status.