

Updates to DTN Node ID Validation and PKIX Profile

Brian Sipos

JHU APL

September 2021 ACME interim



Last Draft Edits

- Changes are in [draft-ietf-acme-dtnnodeid-05](#).
- Main changes:
 - Inherited PKIX profile changes from TCPCLv4 draft, moved claim from SAN URI to SAN otherName with new Name Form.
 - Changed ACME claim identifier from “uri” to “bundleEID” to conform to profile.
- Additional changes:
 - Clarified inherited security considerations and out-of-scope messaging.
 - Clarified entity diagram and fixed typos.
 - Clarified reuse of DNS-ID definition.
- No changes to on-the-wire bundle encoding or logic.
- No changes to ACME logic outside of claim/identifier.

Open Issues from Feedback

- This ACME document still updates a to-be-RFC DTN WG document.
 - This will be resolved by moving the update to an intermediate DTN WG draft, and using that as a normative reference.
 - The overall change is identical to current document, a bookkeeping clarification for BP agent implementers.
- There appear to be a few remaining references to “SAN URI” which should be scrubbed and replaced with accurate text.
 - No other review comments have been received yet.