JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Status of WG and Personal Drafts

IETF 124 DTN WG

Brian Sipos
JHU/APL

Current WG Drafts

- BPSec COSE Context (draft-ietf-dtn-bpsec-cose-10)
- BP EID Patterns (draft-ietf-dtn-eid-pattern-03)
- UDPCLv2 (draft-ietf-dtn-udpcl-01)
- BP SAND (draft-ietf-dtn-bp-sand-01)

BPSec COSE Context

- Completed WG last call with comments captured in GitHub issues
- Changes in -09:
  - Fixed terminology from “security acceptor” to “security verifier or acceptor” to be more accurate
  - Added security consideration “AAD-Covered Block Modification” with requirements about AAD coverage
- Changes in -10:
  - Expanded interoperability algorithm table with variety of security strengths (similar to RFC 9173 scope)
  - Clarified that `COSE_Mac` (multiple recipients) and `COSE_Sign` (multiple signatures) are acceptable in this profile
  - Replaced deprecated ECDSA/EdDSA algorithms with “fully-specified” forms from RFC-to-be 9864
  - Added conformance hints for FIPS 140 and CNSA 1.0 and 2.0
  - Added informative table of header parameters needed for the interop. Algorithms
  - Added explicit section for “Symmetric Keys and Identifiers” to discuss `kid` and `kid context`
  - Updated example base bundle to have a nonzero creation time
  - Added example certificates appendix to clarify the Section 4 PKIX profile

BPSec COSE Context (continued)

- Open issues:
  - PKIX certificate profile discrepancies (#66)
  - Too many required algorithms in Table 5 (#68)
  - Required and Recommended in Table 5 is misleading (#69)
- Open discussion points:
  - What should be the interoperability minimum?
    - This document cannot cover everyone's situation (*e.g.* EdDSA common in IoT)
    - Organize into sections / tables by family (symmetric, NIST ECC, Ed ECC, RSA, ML)?
    - Security strength below CNSA 1.0 minimum?
    - ML-DSA in COSE is now past IESG review, required by CNSA 2.0
  - Is there value in pointing to pending future COSE capabilities in this document?
    - It seems like this is discouraged in IETF standard track documents
    - C509 Certificates, Hash Envelope, ML-DSA, FN-DSA, SLH-DSA, ML-KEM, HPKE

BP EID Patterns

- Provides a framework for patterns on future EID schemes (*e.g.* IMC, IAC)
  - Adds a column to the IANA table to refer to the scheme-specific-pattern-defining specification
- Has multiple implementations from different orgs. in different languages
- Current variations for:
  - Any-scheme matching `*:**`
  - Any-SSP matching `ipn:**`
  - IPN scheme-specific patterns, including wildcard and ranges of each element number
- No DTN scheme-specific patterns specified
- Changes in -03:
  - Altered the recommended EID embedding to match what is already in the Previous Node block content:
    `embed-eid-structure = bstr .cbor eid-structure`
- **No open** discussion points
- Would like a WG last call on the draft as-written

UDPCLv2

- Has had one trial implementation of all features
- Adds extensibility, segmentation, and transport security capabilities
- Includes compatibility mechanisms for:
  - In-band congestion control (IP ECN feedback)
  - IP path MTU probing
  - Limited forms of other IP path characterization (reachability)
- Open discussion points:
  - Need better explanation for extension support not mandatory-to-use
  - Editorial updates are needed to explain extensions
  - Would like to get feedback on the technical mechanisms

BP Secure Advertisement and Neighborhood Discovery

- This draft is attempting to define what transport-agnostic and baseline-secure discovery should look like
- Depends on:
  - UDPCLv2 for **zero-configuration** discovery
  - IMC multipoint scheme for **non-specific** advertisement
  - BP EID Patterns for registered endpoint advertisement
- Advertising capabilities:
  - Credentials (public key certificates)
  - Underlayer networks
  - CLA support
  - Resources (short-horizon power schedule)
  - Local topology (one-hop neighbors, routing metrics)
  - Routing willingness
  - Registered endpoints
- Open discussion points:
  - Needs more implementation experience, specifically for fields needed for neighbor discovery
  - Depends on TBAs in the (not yet defined) IMC endpoint scheme
  - Need discussion about how/if to expose multiple underlayer networks in a single advertisement (#13)

Current Personal Drafts

- BP Security Associations with Few Exchanges (SAFE) (draft-sipos-dtn-bp-safe)
  - This first individual draft provides a starting point for discussion
  - The initialization with EDHOC and primary SA agreement are in a good state
  - Need implementation experience for specific secondary SA use cases
- BP Edge Node with Zero-Configuration (draft-sipos-dtn-edge-zeroconf)
  - Goal is to allow using a BPA in a stable IP (v4 and/or v6) LAN without spending time configuring nodes
    - Allow BP application demos to focus on *using the apps* not on configuring the network
  - This is a purely informational document for how to use existing mDNS and DNS service discovery
  - Could be updated to include additional example of using existing UDPCL service name
  - A proof of concept was implemented in the dtn-demo-agent
  - Is there any interest from BPA implementers to demonstrate “plug and play” mDNS use?