JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

BPSec COSE Context

IETF 121 DTN WG

Brian Sipos
JHU/APL

Status

- BPSec Default Security Contexts are intentionally limited in scope
- For compliance with and integration with existing security infrastructure there is a need for PKI-integrated security
  - This was indicated by IETF SECDIR review of BPSec draft and also discussed as a near-future need by NASA and IOAG DTN planning
- COSE Context draft (draft-ietf-dtn-bpsec-cose-04) has not changed since last IETF
- The current draft has been implemented and privately tested for interoperation (between a C/C++ BPA and a Python BPA each with COTS COSE and crypto libraries).

Next Steps

- This is not intended to replace or supersede existing BPSec interoperability contexts in RFC 9173
- An early allocation of BPSec Context ID has been requested
  - This allows interop testing and diagnostic tooling (e.g. Wireshark)
- Document is ready to proceed out of DTN WG to IESG review
  - There has already been an informal COSE WG review

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Status of Personal Drafts

IETF 121 DTN WG

Brian Sipos
JHU/APL

Current Personal Drafts

- EID Patterns (draft-sipos-dtn-eid-pattern-03)
  - Closest draft to being ready, has multiple implementations
  - DTN scheme has been removed due to its uncertainty and possible complexity
- UDPCLv2 (draft-sipos-dtn-udpcl-02)
  - Has had one trial implementation of all features
  - Adds extensibility and segmentation capability
  - Includes a secondary menu of useful extensions, any of these can be deferred to follow-on draft(s)
  - Relates to BP demux (draft-taylor-dtn-demux-02) and Zero-Config for UDP service name
- BP SAND (draft-sipos-dtn-bp-sand-00)
  - This is a first draft attempting to define what transport-agnostic and secure discovery can look like
  - Depends on UDPCLv2 and EID Patterns
- Edge Node Zero-Config (draft-sipos-dtn-edge-zeroconf-01)
  - This is fully procedural draft, no new protocol and no code point allocations
  - Has had some experimentation but no interoperation testing

Next Steps

- Adoption of the EID Patterns and UDPCLv2, with follow-on detail discussion and feedback, would enable other higher-level BPv7 protocols
  - BP SAND needs both of these
  - A yet-unpublished draft for BP security association management will also rely on EID Patterns
- The UDPCLv2 draft can be tailored and trimmed/split as necessary to make progress toward Proposed Standard
  - UDP port consistency is important for real networks (firewall and NAT traversal, etc.)
  - The Extension Support, Transfer, and security are critical capabilities
  - The path characterization and ECN extensions/procedures are helpful in a non-trivial network but not critical
- Discussion of BP SAND and how it fits into the BPv7 ecosystem
  - IPv6 NDP/SEND operates on ICMPv6 directly on the IP node
  - MANET NHDP operates on UDP above IP