JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

BPSec COSE Context

IETF 120 DTN WG

Brian Sipos
JHU/APL

Background

- BPSec and its Default Security Context are usable but intentionally limited in scope:
  - A limited number of symmetric-keyed encryption and MAC algorithms
  - Defines a narrow-scoped additional authenticated data (AAD) binding to the block/bundle
  - No explicit key identifiers are available
- For internet-facing nodes, possibly as subnetwork gateways, 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
- Don’t want to reinvent the wheel, and CBOR Object Signing and Encryption (COSE) already provides syntax and semantics for current and future PKI security
  - Even COSE (with a restricted profile as used here) still provides a lot of variability, in the same sense that TLS or S/MIME does, which must be managed out-of-band (e.g. don’t use ECC algorithms if security acceptors can’t support it)

Last Changes

- The -04 revision updated the document to address issues
  - #23 No minimum interoperability for x5t algorithms
  - #24 No allowance for single-layer encryption with direct CEK
  - #25 No recommended algorithm for non-wrapped ECDH algorithms
  - #26 Recommend against using PartyU/PartyV
  - #27 Consider bstr-wrapping unbounded size parameters
  - #29 Clarify uses of "security acceptors“
- Only #27 has an effect on the security context processing
  - Change is to use bstr-wrapping of potentially large security parameters to avoid duplicate processing between BPSec engine and Security Context

Next Steps

- This is not intended to replace or supersede existing BPSec interoperability contexts in RFC 9173
- This security context allows BPSec in a ‘traditional’ PKIX environment in the very near term
- This document doesn’t address what kinds of policy are required in a BPA/BPSec implementation
  - There is ongoing work funded by NASA AMMOS which addresses BPSec policy design and implementation
- Document may need another WG Last Call after one last substantive change