JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Bundle Protocol Version 7 Administrative Record Types Registry

IETF 114 DTN WG

Brian Sipos
JHU/APL

Need For this Updating Document

- RFC 7116 created a sub-registry of Administrative Record Types
  - This table is missing the CCSDS Aggregate Custody Signal allocation
- RFC 9171 defines an explicit table of Admin. Record Types
  - Other pre-existing IANA sub-registries with BPv6-7 overlap were updated to include a “Bundle Protocol Version” column, which disambiguates and allows for overlapping registrations
- This proposed document updates the Admin. Record Types sub-registry to be similar to the others with BPv6-7 overlap
  - It makes an explicit reservation of code point zero
  - It adds a high-valued reservation for private or experimental use in the 32-bit-encoded range. This leaves the full 16-bit space available for BPv7 use.
- No change is made to the “Specification Required” registration procedure
  - An existing comment #1 recommends to make this “no change” explicit

What the Changes Look Like

Bundle Protocol Version	Value	Description	Reference
6,7	0	Reserved	[RFC7116] [This specification]
6,7	1	Bundle status report	[RFC5050] [RFC9171]
6	2	Custody signal	[RFC5050]
6,7	3	Unassigned	
6	4	Aggregate Custody Signal	[CCSDS-BP]
6,7	5-15	Unassigned	

Bundle Protocol Version	Value	Description	Reference
7	16-65535	Unassigned	
7	greater than 65535	Reserved for Private or Experimental Use	This specification

Next Steps

- Requesting the DTN WG to adopt this document
- This would eventually be in a cluster with the ACME document registering the new code point
- The BIBE document would also eventually need code points

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

BPSec COSE Context

IETF 114 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 variable 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 DTN planning group.
- 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).
  - Planning is already underway for hybrid public key encryption (HPKE) and post-quantum cryptography (PQC).

Proposed COSE Context Contents

- One BPSec context codepoint defined to use in BIB and BCB.
- Parameter and result types defined for each BPSec block type:
  - AAD scope parameter (same semantics as Default SC)
  - De-duplicated last-layer COSE header parameters.
  - Integrity results (COSE MAC and Signature)
  - Confidentiality results (COSE Encrypt using AEAD)
- Public keys in context parameters to de-duplicate data.
  - Potential future extensions could provide additional supporting data (e.g. OCSP stapling).
- Full COSE messages contained in each target's result.
  - Reuse COSE message tags as result type codes.
  - Allows an application to use any current or future COSE algorithm types (and combinations).
  - Allows multiple recipients for a single security block (both BIB and BCB).
  - Interoperability requirements are defined in a COSE Profile (next slide).

Interoperability Profile

- Required algorithms for AES-GCM-256, AES key-wrap, and HMAC-SHA2-256.
- Recommended algorithms for Elliptic Curve, Edwards Curve, and RSA signing and key-wrap/key-generation.
- Additional public key material can be included in an “additional header map”, applying to all results in the block.

BPSec Block	COSE Layer	Name	Code	Implementation Requirements
Integrity	1	HMAC 256/256	5	Required
Integrity	1	ES256	-7	Recommended
Integrity	1	EdDSA	-8	Recommended
Integrity	1	PS256	-37	Recommended
Confidentiality	1	A256GCM	3	Required
Confidentiality	2	A256KW	-5	Required
Confidentiality	2	ECDH-ES + A256KW	-31	Recommended
Confidentiality	2	ECDH-SS + A256KW	-34	Recommended
Confidentiality	2	RSAES-OAEP w/ SHA-256	-41	Recommended

Table 5: Interoperability Algorithms

Next Steps

- This is not intended to replace or supersede existing symmetric-keyed BPSec interoperability contexts in RFC 9173.
- The point here is to allow BPSec in a PKIX environment in the very near term.
  - COSE is a known quantity with existing coding and processing tools.
  - Identifying bundle security purpose and validation of a Node ID within a PKIX certificate are already defined in RFC 9174.
  - An extension to ACME to automate validation of a Node ID is under review.
- Known changes needed:
  - #10 Align AAD encoding with RFC 9173 for consistency.
- Some secondary questions remain, for example:
  - How does a security acceptor handle a BIB signed by a key with a certificate for a different Node ID than the security source? Base BPSec doesn't really deal with identity/authentication logic.
  - Is there a more strict minimum COSE header content? S/MIME makes requirements about full certificate presence, while the current draft allows an "x5t" thumbprint as a placeholder for compact encoding.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Neighbor Messaging and Discovery

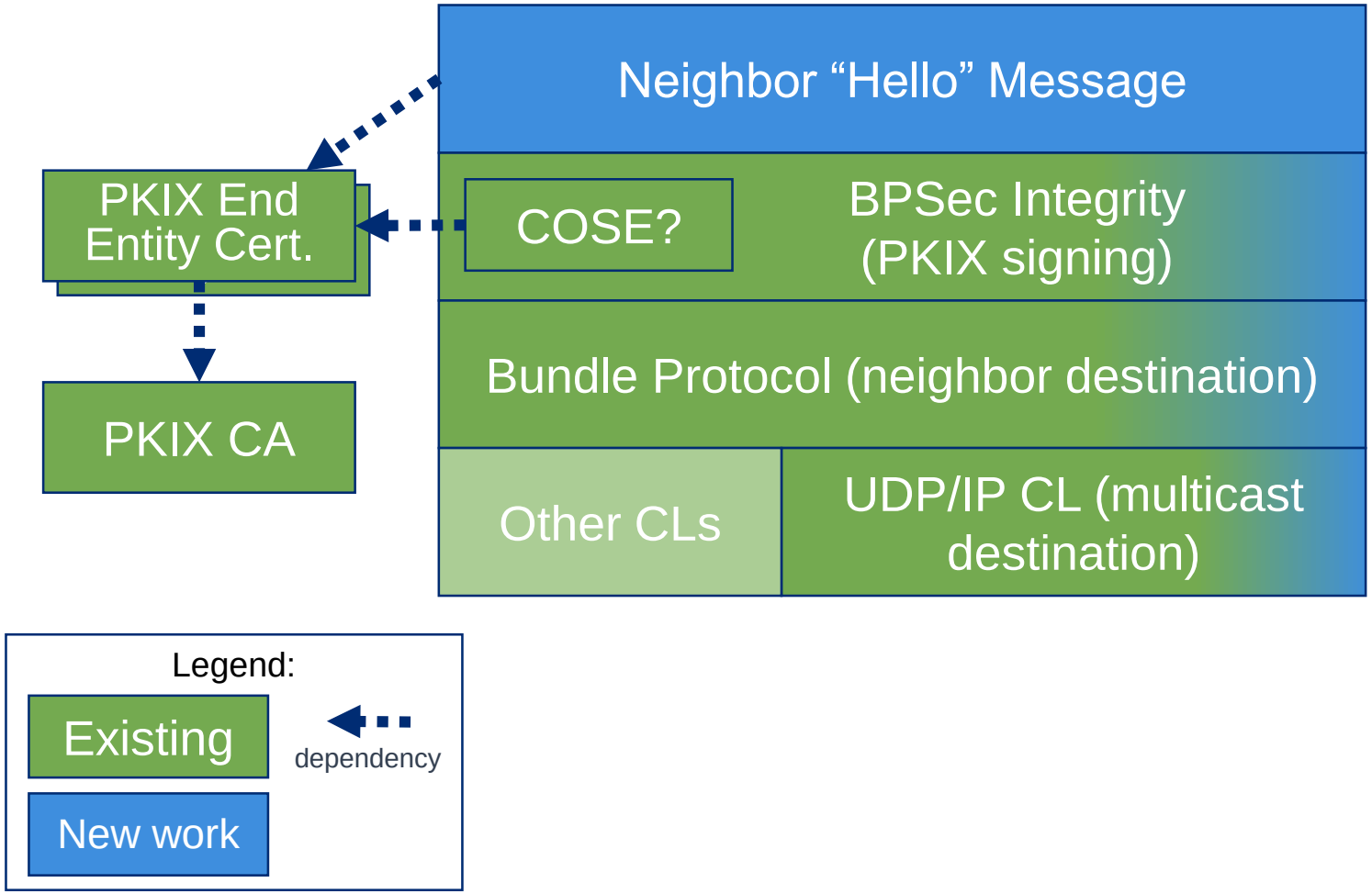
IETF 114 DTN WG

Brian Sipos
JHU/APL

Background

- Current WG charter includes a “Neighbor/Peer Discovery Protocol” milestone
- Existing IRTF experimental draft for IPND is narrow in scope and not extensible to different transport/network or to have security
- An existing need for authenticated discovery is present in discussions of future automation
  - Use cases in Step 3 and 4 of DNAC presentation (CL#19-7832.pdf)
- Similar concepts already exists in MANET NHDP, which include
  - Abstract messaging over multicast UDP/IP
  - Hello message definition with network address and route TLVs
  - Integrity and group authentication with MAC TLV
- Much of the proposed infrastructure already exists in the BPSec/BPA/CLA stack

Proposed Neighbor Messaging Stack



Neighbor Messaging Details

- A “neighbor” is a one-hop bundle destination
- A “neighbor bundle” is a bundle addressed to a sentinel EID
  - In the same way “dtn:none” is the anonymous source, this proposes “dtn:~neighbor” as an non-specific destination EID
- The payload of a neighbor bundle is a CBOR map with labels defined in a registry, similarly to existing protocols (e.g. COSE, CORECONF)
  - MANET messaging (RFC 5444) also uses similar logic but different encoding
- Allows reuse of existing BP and BPSec tools:
  - Neighbor bundles can be transported over any CLA (or multiple if useful)
  - BPSec allows easily adding security that IPND lacks and other protocols bolted-on later in their design
  - Bundle lifetime, Previous Node, and Hop Count control distribution and retention of the individual message (similar to MANET message parameters)

Neighbor Hello Message

- The Hello message is equivalent to a MANET NHDP or IRTF IPND beacon
  - It is sent unsolicited, based on some long-period timer or link status event
  - It is encoded as a Neighbor Message (CBOR map)
- By definition a bundle with a Hello message has a one-hop limit and a last hop Node ID identical to its source Node ID
  - Other neighbor message types can have similar restrictions
- The Hello identifies aspects of the bundle source which are useful to other members of its “local” one-hop overlay network:
  - Any alias Node IDs of the node (if it has other names)
  - Cryptographic binding of the Node IDs (e.g. PKIX end-entity certificate)
    - Including this in the payload instead of BIB allows bundle fragmentation
    - Multiple certificates can be present, separating signing and encryption keys
  - What CLs are available on the node, and what is their coarse schedule
    - This includes both passive (listening) and active (sending) CLAs
  - Which one-hop neighbors are already known to the sending node
  - Others TBD with private/experimental reservation
  - Could include the concept of an EID pattern for route advertisement

The `dtn:~neighbor` Destination EID

- This well-known scheme specific part (SSP) extends the existing EID definition from “dtn:none”
  - This EID can have a similar compressed encoding from text “~neighbor” to integer value
- This well-known EID will be handled
- This SSP conforms to existing URI handlers as a path-only URI
- The tilde conforms to existing “dtn” scheme logic for multicast service naming

Messaging Security

- The abstract concept requires no specific security context(s) but certain capabilities will constrain what contexts are useful
- There are currently no defined BPSec contexts which allow signing with asymmetric keys (e.g. within a PKI)
  - There is a proposal for a COSE Security Context which would allow PKIX signature and reference to end-entity certificate by thumbprint
- The BIB signing the primary+payload blocks can also function as authentication if tied to an identity (e.g. a PKIX certificate chained to a trusted CA)
  - The CA vouches for the certificate's subject-alternative-name bundleEID
  - The public key in the certificate verifies the BIB signature
  - The BIB covers the primary block and its Source Node ID to authenticate it
  - Also the BIB covers the payload block to ensure its integrity

Neighbor-Reaching Convergence Layers

- Unlike IPND, this proposed stack uses bundle framing so can be transported over any CL available to the BPA
- Some link-specific unicast CLs can use neighbor Hello messaging as a handshake or keepalive mechanism
  - For example, in a closed network known to use LTPCL a newly available peer (found via DLEP, NHDP, OLSR, etc.) can be probed with a Hello message over LTP
- Other broadcast/multicast CLs can use Hello messaging for unsolicited node discovery
  - This would make use of a Proposed Standard UDPCL (mentioned to the WG in earlier IETFs) that is compatible with the IRTF Experimental UDPCL but with some aspects constrained for interoperability

Next Steps

- Requesting the DTN WG to consider this concept and related documents:
  - A very boilerplate neighbor messaging draft exists on Github, hasn't been touched for over a year
  - BPSec COSE Context for PKIX signing and authentication
  - UDPCL standardization for multicast transfers and bundle version detection