JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road
Laurel, MD 20723-6099

IETF 111 DTN WG

Updates to the Default Security Contexts

Edward J. Birrane, Ph.D.
Johns Hopkins University, Applied Physics Laboratory (JHU/APL)

History and Review

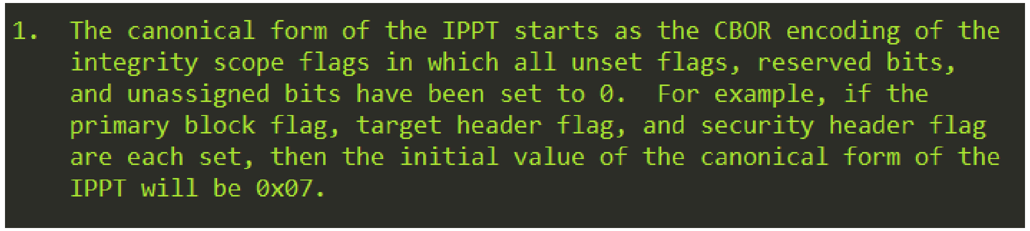
- -07 drafted on May 17th
  - Some AD comments received about adding registry for scope flags and clarifying authentication tag
- -08 drafted on June 8th
  - Submitted for IESG Review
  - Several comments received.
- -09 drafted on July 8th
  - Solicit feedback from IESG reviewers. This solves most comments
- -10 drafted on July 12th
  - Corrected some typos/syntax errors
  - Cleared IESG review
    - 2 YES
    - 10 No Objection
    - 2 No Record

Default Security Context Changes

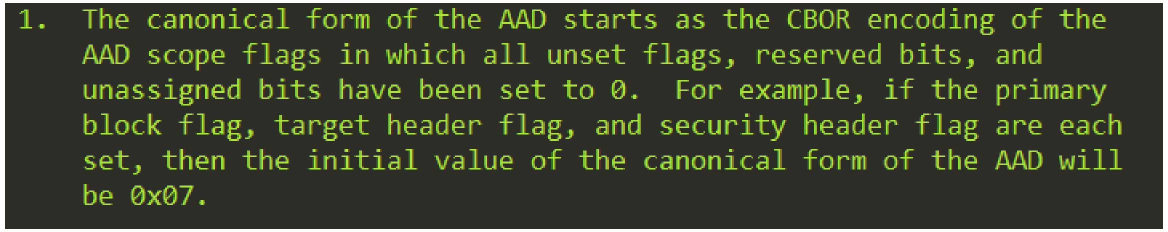
- Editorial
  - Fixed some typos in bit values, terms for CBOR types
  - Updated some references as requested by reviewers
  - Added some text referencing back to BPv7 and BPSec to help readers with definitions

Normative Changes

- IPPT and AAD
  - IPPT and AAD scope flags MUST be included in the values they generate.
  - IPPT and AAD scope flag unset and reserved and unassigned bits must be set to 0
  - Specified width of these fields to be 16 bits.



```
1.  The canonical form of the IPPT starts as the CBOR encoding of the
    integrity scope flags in which all unset flags, reserved bits,
    and unassigned bits have been set to 0.  For example, if the
    primary block flag, target header flag, and security header flag
    are each set, then the initial value of the canonical form of the
    IPPT will be 0x07.
```



```
1.  The canonical form of the AAD starts as the CBOR encoding of the
    AAD scope flags in which all unset flags, reserved bits, and
    unassigned bits have been set to 0.  For example, if the primary
    block flag, target header flag, and security header flag are each
    set, then the initial value of the canonical form of the AAD will
    be 0x07.
```

- Key Wrap
  - Specified that wrapped keys use AES Key Wrap (AES-KW) from RFC5649
- Authentication Tag
  - Tag can be either in a security result or combined with the generated cipher text (but not both)

Informative Changes

- Clarifications
  - Clarify: Keys cannot be used across security contexts. Same for KEKs.
  - Updated examples of removing BP CBOR encodings when generating canonical forms
  - Several clarifications around how to handle the authentication tag, since it could be a security result or generated with the cipher text
- Guidance
  - Noted padding not needed for AES key wrap because of allowable key lengths.
  - A significant amount of educational text around the proper use of cipher suites and pointers to relevant documents from NIST and IETF.
    - Lots of text focusing on uniqueness of per-invocation IVs
    - Text on constant-time comparisons for integrity verification
    - Upper bound on number of encryption invocations performable by the same key
    - Same constructions for generating unique IV values
    - Upper bound on the number of AES blocks that can be processed by the same key
  - Added section 5.4 “Guidance for Designated Experts”
    - When processing new scope flag requests.
  - Added Appendix A – Examples of security block processing (21 pages)
  - Added Appendix B – Example CDDL for the IPPT and AAD flags.