BPSec,
Interoperabilty Cipher Suites

IETF-104

Edward Birrane

Edward.Birrane@jhuapl.edu

443-778-7423

APL

JOHNS HOPKINS UNIVERSITY

Applied Physics Laboratory

Overview

- BPSec
  - Updates from Last DTNWG.
  - Updates from CCSDS review.
  - Discussion points
- Interoperability Cipher Suites
  - Updates
- Open questions

BpSec Updated from IETF 103 (1/2)

1. Should we add a “Security Associations Block” As requested by CCSDS
   - No. Abstract Cipher Suite verbiage instead.

2. No other real changes.

BpSec Updated from IETF 103 (2/2)

1. Added definition of Cipher Suite
2. Added definition of Security Context
3. Changed instances of cipher suite (id, parms, results) to security context (id, parms, results)
4. Removed all references and description of the proposed “security associations” block.
5. Added some additional examples for a security context
6. Removed redundant text associated with BCBs whose cipher text is not the same size as the plain text.

CCSDS SEA-SEC Review Comments

- BPSec-09 judged as “very good
- Comments:
  - Concur: Section 1.1 – you say that integrity services “ensure” that target data within in a bundle are not changed… Not really true. Integrity ensures that if there are any changes, they are discovered.
  - Concur: Section 1.4 – add CBOR to the terminology list
  - Concur. Section 3.2 – why not just say that no nesting is allowed?
  - No Change. Section 3.6 – why are the security source and context parameters optional? Is the Security Results field meant to be meta-data to indicate the services applied?
    - *Not every context is parameterized.*
  - No Change. Section 3.9 – here’s where you say that authenticated encryption is used in BCB. I’d suggest that this be made clear someplace in the introductory material up front. This should also be a SHALL statement and not just a NOTE.
    - *The MUST statement does exist in section 3.8.*

Interoperability Cipher Suites

- Changes terminology from “cipher suite” to security context
- Updated references
- Submitted as WG document (not personal draft)