JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

BPSec Updates

IETF-109

Ken McKeever
Ken.McKeever@jhuapl.edu
240-228-2237

BPSec Current Status

- Summary
  - https://datatracker.ietf.org/doc/draft-ietf-dtn-bpsec/ballot/
  - Genart – Editorial comments, all resolved
  - IANA – No issues

- Yes
  - B. Kaduk
  - M. Westerlund
- No Objection
  - D. Brungard, A. Cooper, R. Danyliw, B. Leiba, A. Retana, E. Vyncke
- Discuss
  - M. Kühlewind
  - Remaining item regarding mandatory security context(s); believed to be addressed in BPSec-24

- BPSec, BPBis (BPv7), and TCPCLv4 will be on the telechat for first week of December

Updates Since IETF-108

#	Question	Updates made in BPSec-24?	Functional Change in BPSec-24?
1	**Should there be one security context that is considered "Mandatory to Implement" (MTI) for all BPSec implementations?**	**Yes**	**Yes**
2	Can BPSec be standardized absent a key exchange protocol?	No	No
3	**Consider allowing nested signatures.**	**Yes**	No
4	**Consider signature or encryption over multiple blocks.**	**Yes**	No
5	**Bundle Protocol Reason Codes**	**Yes**	**Yes**
6	Should BPSec encode security context parms as a CBOR Map?	No	No
7	Should BPSec force integrity of non-block-type-specific data?	No	No
8	**Should BPSec reserve some security context parm/result ids to promote commonality?**	**Yes**	**Yes**

BPSec Open Question #1

- Should there be one security context that is considered “Mandatory to Implement” (MTI) for all BPSec implementations?
  - BPSec-22 did not mandate a security context
  - BPSec-24 has been updated to mandate support (at a minimum) for default security context(s)
  - BPSec-24 maintains requirement for implementations to support security context(s) within operating networks

To ensure interoperability among various implementations, all BPSec implementations MUST support at least the current IETF standards- track mandatory security context(s). As of this writing, that BCP mandatory security context is specified in [I-D.ietf-dtn-bpsec-interop-sc], but the mandatory security context(s) might change over time in accordance with usual IETF processes. Such changes are likely to occur in the future if/ when flaws are discovered in the applicable cryptographic algorithms, for example.

Additionally, BPsec implementations need to support the security contexts which are specified and/or used by the BP networks in which they are deployed.

BPSec Open Question #3

- Consider allowing nested signatures.
  - No functional change from BPSec-22
  - Added language to BPSec-24 to recommend implementation through custom security context and/or custom security blocks

The security blocks defined in this specification (BIB and BCB) are designed with the intention that the BPA adding these blocks is the authoritative source of the security service. If a BPA adds a BIB on a security target, then the BIB is expected to be the authoritative source of integrity for that security target. If a BPA adds a BCB to a security target, then the BCB is expected to be the authoritative source of confidentiality for that security target. More complex scenarios, such as having multiple nodes in a network sign the same security target, can be ***accommodated using the definition of custom security contexts (Section 9) and/or the definition of other security blocks (Section 10).***

BPSec Open Question #4

- Consider signature or encryption over multiple blocks.
  - No functional change from BPSec-22
  - Added language BPSec-24 to recommend implementation through custom security context

Since OP(bib-integrity, target) is allowed only once in a bundle per target, it is RECOMMENDED that users wishing to support multiple integrity mechanisms for the same target define a multi- result security context. Such a context could generate multiple security results for the same security target using different integrity-protection mechanisms or different configurations for the same integrity-protection mechanism.

A BIB is used to verify the plain text integrity of its security target. However, a single BIB MAY include security results for blocks other than its security target when doing so establishes a needed relationship between the BIB security target and other blocks in the bundle (such as the primary block).

BPSec Open Question #5

- Bundle Protocol Reason Codes
  - A BP Node may discard a bundle for security reasons.
  - BPSec-24 defines reason codes to be included in status reports:
    - Missing Security Service: Required service not present in bundle at waypoint or acceptor.
    - Unknown Security Service: Unknown context, parameter, etc… at waypoint/acceptor.
    - Unexpected Security Service: More security in bundle than expected.
    - Failed Security Service: Failed to verify integrity or decrypt a services at waypoint or acceptor.
    - Conflicting Security Service: security blocks violate BPSec rules.
  - Allocates five reason codes from the existing "Bundle Status Report Reason Codes" registry defined in [RFC6255].

BPSec Open Question #8

- Should BPSec reserve some security context parm/result ids to promote commonality?
  - BPSec-24 sets negative values as reserved for local or site-specific use in the Security Context Identifier Registry

BPSec Security Context Identifier Registry

Value	Description	Reference
< 0	Reserved	This document
0	Reserved	This document

Table 3

Negative security context identifiers are reserved for local/site- specific uses. The use of 0 as a security context identifier is for non-operational testing purposes only.

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY