Delay-Tolerant Networking
Internet-Draft
Intended status: Standards Track
Expires: December 26, 2020

B. Sipos
RKF Engineering

June 24, 2020

DTN Bundle Protocol Security COSE Security Contexts
draft-bsipos-dtn-bpsec-cose-00

Abstract

This document defines an integrity security context and a confidentiality security context suitable for using CBOR Object Signing and Encryption (COSE) algorithms within Bundle Protocol Security (BPSec) blocks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 26, 2020.

Table of Contents

1. Introduction

The Bundle Protocol Security (BPSec) Specification [I-D.ietf-dtn-bpsec] defines structure and encoding for Block Integrity Block (BIB) and Block Confidentiality Block (BCB) types but does not specify any security contexts to be used by either of the security block types. The CBOR Object Signing and Encryption (COSE) specification [RFC8152] defines a structure, encoding, and algorithms to use for cryptographic signing and encryption.

This document describes how to use the algorithms and encodings of COSE within BPSec blocks to apply those algorithms to Bundle security. A bare minimum of interoperability algorithms and algorithm parameters is specified by this document.

This document does not address how those COSE algorithms are intended to be used within a larger security context.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP

14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. BPSec Security Contexts

Rather than defining a single security context for both integrity and confidentiality blocks, this document specifies two separate security contexts which are analogous to the two BPSec block types. Each security context allows a specific set of BPSec Result IDs.

The existing COSE structure-marking tags in Section 2 of [RFC8152] SHALL be used as BPSec Result ID values for all COSE security contexts (see Table 1 and Table 2). This avoids the need for value-mapping between code points of the two registries.

When embedding COSE structures, the CBOR-tagged form SHALL NOT be used. The Result ID values already provide the same information as the COSE tags.

3.1. COSE Integrity Context

The COSE Integrity Context has a Security Context ID of TBD-CI.

The integrity context SHALL allow only the Result IDs from Table 1. Each integrity context result value SHALL consist of the COSE structure indicated by Table 1 in its decoded form.

Result ID	Result Structure
97	COSE_Mac
17	COSE_Mac0
98	COSE_Sign
18	COSE_Sign1

Table 1: COSE Integrity Results

Each integrity result SHALL use the "detached" payload form with nil payload value. The integrity result for COSE_Mac and COSE_Mac0 structures are computed by the procedure in Section 6.3 of [RFC8152]. The integrity result for COSE_Sign and COSE_Sign1 structures are computed by the procedure in Section 4.4 of [RFC8152].

[NOTE: This differs from base BPSec in that the entire block and the bundle primary is signed] The COSE "payload" used to generate a signature or MAC result SHALL be the canonically serialized target block, including the canonical block array structure. The COSE "protected attributes from the application" used to generate a signature or MAC result SHALL be either:

For a primary block target: An empty byte string.

For a canonical block target: The canonically serialized primary block of the bundle.

3.1.1. Interoperability Algorithms

[NOTE: This is identical to the [I-D.ietf-dtn-bpsec-interop-sc] minimum list.] The minimum set of integrity algorithms needed for interoperability is listed here. The full set of algorithms available is managed at [IANA-COSE].

Name	Code
HMAC 256/256	5

Integrity Algorithms

3.2. COSE Confidentiality Context

The COSE Confidentiality Context has a Security Context ID of TBD-CC.

The confidentiality context SHALL allow only the Result IDs from Table 2. Each confidentiality context result value SHALL consist of the COSE structure indicated by Table 2 in its decoded form.

Result ID	Result Structure
96	COSE_Encrypt
16	COSE_Encrypt0

Table 2: COSE Confidentiality Results

Only algorithms which support Authenticated Encryption with Authenticated Data (AEAD) SHALL be usable in the first (content) layer of a confidentiality result. Because COSE encryption with AEAD

appends the authentication tag with the ciphertext, the size of the block-type-specific-data will grow after an encryption operation.

Each confidentiality result SHALL use the "detached" payload form with nil payload value. The COSE plaintext and ciphertext correspond exactly with the target block-type-specific-data. The confidentiality result for COSE_Encrypt and COSE_Encrypt0 structures are computed by the procedure in Section 5.3 of [RFC8152].

[NOTE: This differs from base BPSec in that AAD from the block and the bundle primary is used] The COSE "plaintext" used to generate an encrypt result SHALL be the block-type-specific-data of the target block, the decoded byte string itself (not including the encoded CBOR item header). The COSE "protected attributes from the application" used to generate an encrypt result SHALL be the concatenation of the following:

1. The canonically serialized primary block of the bundle.

2. The canonically serialized augmented target block, which has its block-type-specific-data substituted with an empty byte string.

3.2.1. Interoperability Algorithms

[NOTE: This is identical to the [I-D.ietf-dtn-bpsec-interop-sc] minimum list.] The minimum set of integrity algorithms needed for interoperability is listed here. The full set of algorithms available is managed at [IANA-COSE].

Name	Code
A256GCM	3

Confidentiality Algorithms

4. Implementation Status

[NOTE to the RFC Editor: please remove this section before publication, as well as the reference to [RFC7942].]

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation

here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations can exist.

5. Security Considerations

This section separates security considerations into threat categories based on guidance of BCP 72 [RFC3552].

All of the security considerations of the underlying BPSec [I-D.ietf-dtn-bpsec] apply to these new security contexts.

5.1. Threat: BPSec Block Replay

The bundle's primary block contains fields which should uniquely identify a bundle: the Source Node ID, Creation Timestamp, and fragment parameters (see Section 4.2.2 of [I-D.ietf-dtn-bpbis]). Including the primary block in the AAD for integrity and confidentiality binds the verification of the secured block to its parent bundle and disallows replay of any block with its BIB or BCB.

This profile of COSE limits the encryption algorithms to only AEAD in order to include the context of the encrypted data as AAD. If an agent mistakenly allows the use of non-AEAD encryption when decrypting and verifying a BCB, the possibility of block replay attack is present.

5.2. Threat: Algorithm Vulnerabilities

Because this use of COSE leaves the specific algorithms chosen for BIB and BCB use up to the applications securing bundle data, it is important to use only COSE algorithms which are marked as recommended in the IANA registry [IANA-COSE].

6. IANA Considerations

Registration procedures referred to in this section are defined in [RFC8126].

6.1. BPSec Security Contexts

Within the "Bundle Protocol" registry [IANA-BUNDLE], the following entry has been added to the "BPSec Security Context Identifiers" sub-registry.

Value	Description	Reference
TBD-CI	COSE Integrity	This specification.
TBD-CC	COSE Confidentiality	This specification.

7. Acknowledgments

The interoperability minimum algorithms and parameters are based on the draft [I-D.ietf-dtn-bpsec-interop-sc].

8. References

8.1. Normative References

[I-D.ietf-dtn-bpsec]
Birrane, E. and K. McKeever, "Bundle Protocol Security Specification", draft-ietf-dtn-bpsec-22 (work in progress), March 2020.

[IANA-BUNDLE]
IANA, "Bundle Protocol", <https://www.iana.org/assignments/bundle/>.

[IANA-COSE]
IANA, "CBOR Object Signing and Encryption (COSE)", <https://www.iana.org/assignments/cose/>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[I-D.ietf-dtn-bpbis]
Burleigh, S., Fall, K., and E. Birrane, "Bundle Protocol Version 7", draft-ietf-dtn-bpbis-25 (work in progress), May 2020.

[I-D.ietf-dtn-bpsec-interop-sc]
Birrane, E., "BPSec Interoperability Security Contexts", draft-ietf-dtn-bpsec-interop-sc-01 (work in progress), February 2020.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

Appendix A. Examples

A.1. COSE_Mac0

This is an example of a MAC with implied recipient (and its key material). The two provided figures are CBOR diagnostic notation [RFC7049] of the target block being signed and the Abstract Security Block (which will itself be enveloped within a BIB).

The 256-bit key used is h'13bf9cead057c0aca2c9e52471ca4b19ddfaf4c0784e3f3e8e3999dbae4ce45c'.

```
[
  7, / BP version /
  0, / flags /
  0, / CRC type /
  [1, '//dst/'], / destination /
  [1, '//src/'], / source /
  [1, '//src/'], / report-to /
  [0, 40], / timestamp /
  1000000 / lifetime /
]
```

Figure 1: Primary block CBOR diagnostic

The primary block encodes to h'880700008201462f2f6473742f8201462f2f73
72632f8201462f2f7372632f820018281a000f4240'.

```
[
  7, / type code - bundle age /
  2, / block num /
  0, / flags /
  0, / CRC type /
  h'19012c' / type-specific-data:
    300 \ age \
  /
]
```

Figure 2: Target block CBOR diagnostic

The target data to be signed is concatenated from the primary encoded
and h'85070200004319012c'.

```
[
  [2], / targets /
  0, / security context TBD /
  0, / flags /
  [
    [ / target block #2 /
      [ / result /
        17, / COSE_Mac0 tag /
        [
          h'a10105' / protected {
             \ alg \ 1:5 \ HMAC 256//256 \
           } / ,
          {}, / unprotected /
          null, / payload /
          h'91d5f4025cf5fdaf4979ae288cc4aee85b556d4c8c4a87ba880e2dd0b9dd2219' /
tag /
        ]
      ]
    ]
  ]
]
```

Figure 3: Abstract Security Block CBOR diagnostic

A.2. COSE_Encrypt0

This is an example of an encryption with implied recipient (and its key material). The provided figures are CBOR diagnostic notation [RFC7049] of the target block being encrypted, the Abstract Security Block (which will itself be enveloped within a BCB), and the resulting target block.

The 256-bit key used is h'13bf9cead057c0aca2c9e52471ca4b19ddfaf4c0784e3f3e8e3999dbae4ce45c'.

```
[
  7, / BP version /
  0, / flags /
  0, / CRC type /
  [1, '//dst/'], / destination /
  [1, '//src/'], / source /
  [1, '//src/'], / report-to /
  [0, 40], / timestamp /
  1000000 / lifetime /
]
```

Figure 4: Primary block CBOR diagnostic

The primary block encodes to h'880700008201462f2f6473742f8201462f2f73
72632f8201462f2f7372632f820018281a000f4240'.

```
[
  7, / type code - bundle age /
  2, / block num /
  0, / flags /
  0, / CRC type /
  h'19012c' / type-specific-data:
    300 \ age \
  /
]
```

Figure 5: Initial Target block CBOR diagnostic

The target plaintext is h'19012c' with AAD concatenated from the primary encoded and h'850702000040'. A random IV is generated for this operation and is indicated in a standard way.

```
[
  [2], / targets /
  0, / security context TBD /
  0, / flags /
  [
    [ / target block #2 /
      [ / result /
        16, / COSE_Encrypt0 tag /
        [
          h'a10103', / protected {
             \ alg \ 1:3 \ A256GCM \
           } /
          { / unprotected /
            / iv / 5: h'6f3093eba5d85143c3dc484a'
          },
          null / payload /
        ]
      ]
    ]
  ]
]
```

Figure 6: Abstract Security Block CBOR diagnostic

```
[
  7, / type code - bundle age /
  2, / block num /
  0, / flags /
  0, / CRC type /
  h'63bb16e3f7440706835f460dabc29e9dfc4284' / ciphertext /
]
```

Figure 7: Encrypted Target block CBOR diagnostic

Author's Address

Brian Sipos
RKF Engineering Solutions, LLC
7500 Old Georgetown Road
Suite 1275
Bethesda, MD 20814-6198
United States of America

Email: BSipos@rkf-eng.com