BPSeq COSE Contexts

BRIAN SIPOS
RKF ENGINEERING SOLUTIONS
IETF108
Motivations for COSE Contexts

- BPSec security contexts are tailored to specific situations and optimized for minimum-encoded-size security blocks.
- BPSec focus is on symmetric-keyed algorithms.
- For internet-facing nodes, possibly as subnetwork gateways, there is a need for PKI-integrated security.
  - This was indicated also by SECDIR review of BPSec draft.
- Don’t want to reinvent the wheel, and CBOR Object Signing and Encryption (COSE) already provides syntax and semantics for current and future security algorithms.
Goals for Contexts

• No not alter BPSec structures or requirements.
  • This is purely an extension within the existing security context mechanism.
• Handle current symmetric-keyed and PKI algorithms.
  • Leverage existing algorithm definitions.
• Follow algorithm-use and key-use best practices.
  • Avoid key overuse, use random content encryption keys.
• Inherit future gains made by COSE off-the-shelf algorithms.
Proposed Security Contexts

• One new context for each block type:
  • COSE Integrity
  • COSE Confidentiality
• No parameters to the context; each COSE result is self-contained.
• Full COSE messages 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)
  • Interoperability requirements in COSE Profile (next slide)
• Keep it simple!
Proposed COSE Profile

- Required algorithms for AES-GCM-256 and HMAC-SHA2-256.
- Recommended algorithms for EC and RSA signing and key-wrap.

<table>
<thead>
<tr>
<th>BPSeq Block</th>
<th>COSE Layer</th>
<th>Name</th>
<th>Code</th>
<th>Implementation Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>1</td>
<td>HMAC 256/256</td>
<td>5</td>
<td>Required</td>
</tr>
<tr>
<td>Integrity</td>
<td>1</td>
<td>ES256</td>
<td>-7</td>
<td>Recommended</td>
</tr>
<tr>
<td>Integrity</td>
<td>1</td>
<td>PS256</td>
<td>-37</td>
<td>Recommended</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>1</td>
<td>A256GCM</td>
<td>3</td>
<td>Required</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>2</td>
<td>A256KW</td>
<td>-5</td>
<td>Recommended</td>
</tr>
<tr>
<td>Integrity or Confidentiality</td>
<td>2</td>
<td>ECDH-ES + A256KW</td>
<td>-31</td>
<td>Recommended</td>
</tr>
<tr>
<td>Integrity or Confidentiality</td>
<td>2</td>
<td>RSAES-OAEP w/ SHA-256</td>
<td>-41</td>
<td>Recommended</td>
</tr>
</tbody>
</table>

Table 3: Interoperability Algorithms
Clarifications to BPSec drafts

• The current BPSec draft and the interoperability contexts draft does not require either BIB or BCB to include target-block or primary block data in an algorithm’s additional authenticated data (AAD).
  • This allows a trivial reply attack where a block and it’s associated ASB are simply copied from one bundle to another.
  • This kind of replay is mentioned in the security considerations of BPSec but there is no discussion of recommended behavior of security contexts to deal with this threat.

• The COSE contexts require AEAD encryption and require that both BIB and BCB include the primary block and target block metadata as AAD.
  • This binds the security result to that exact block and its containing bundle.

• It means that AAD cannot change after BIB or BCP is applied.
  • The primary block is required to be immutable already.
  • What valid operation would modify target block data? Block types and numbers are also immutable.
Desired WG Direction

• This is not intended to replace or supersede existing BPSEC interoperability contexts ([draft-ietf-dtn-bpsec-interop-sc-01](https://tools.ietf.org/html/draft-ietf-dtn-bpsec-interop-sc-01))

• The point here is to allow BPSEC in a PKI environment in the very near term.
  • COSE is a known quantity with existing coding and processing tools.

• If accepted, requirements and examples could be tightened up.
  • Existing draft should be implementable and testable as-is.
  • Examples come from scripts in the referenced repository.
  • An example of all recommended uses could be provided if desired.