JOSE
Additional feature proposals
Compression

- Currently JWE uses ZLIB, this has header and CRC overhead.
- Change to Deflate?
- Make configurable?
Thumbprint

• SHA1 is the current practice.
• Add thumbprint type parameter?
  • Sniff value?
• add separate parameter for each type?
  • x5t, x5t_HS256, x5t_MD5 etc
Presenter Confirmation

- Should we add a method of doing presenter confirmation such as holder of key?
- Is this a generic feature or better as part of JWT
Key Type

• Add explicit Key Type parameter
Additional Algorithms

• ECDH-SS (Static-Static)
• We have ECDH (Static-Ephemeral)
• Allows for sender verification