COSE: Additional Algorithms

Jim Schaad

August Cellars

Current State

- MAC Algorithms – KMAC --- new
- Key Wrap Algorithms – AES-KW w/ padding
- Key Agreement Algorithms
  - Direct w/ KDF – ECDH w/ KMAC --- new
  - Key Wrap w/ KDF – ECDH w/ KMAC + AES-KW -- new
- Signature Algorithms – none
- Hash Algorithms – none
- Content Encryption Algorithms – none
- Password KDF Algorithms – none

Questions to answer

- What other algorithms (if any) need to be added to this document?
- Is this document ready for adoption call?
- Use this document (plus) github for examples of these algorithms?