JOSE Feature Set

Jim Schaad
August Cellars

Capability List from CMS (1)

- One Pass Processing (I,E)
- Interior Content Identification (I,E)
- Content encoding methods (I,E)
- Parallel Signatures (I)
- Protected Attributes (I,E)
- Unprotected Attributes (I,E)

Capability List from CMS (2)

- Multiple Recipients (I, E)
- Recipient Encryption Methods (I, E)
  - Key Transport (RSA)
  - Key Agreement (ECDH)
    - Static-static, ephemeral-static, ephemeral-ephemeral
  - Pre-Shared Secret w/o Key Derivation
  - Pre-Shared Secret w/ Key Derivation (Password)
  - Other (IBE, Plasma)

Capability List from CMS (3)

- Recipient/Signer Identification (I, E)
- Re-serialization (I)

Discussion?