Updates to JOSE Specifications Since IETF 84

John Bradley
Nov 7, 2012

JSON Web Signature (JWS)

- Normative changes made:
  - Changed `x5c` (X.509 Certificate Chain) from being a single string to being an array of strings, each representing an element of the cert chain

JSON Web Encryption (JWE)

- Normative changes made:
  - Merged `enc`, `int`, and `kdf` into single `enc` header parameter
  - Promoted Initialization Vector from a header parameter to a top-level JWE element

JSON Web Key (JWK)

- Normative changes made:
  - Changed RSA key parameter names `mod` and `exp` to `n` and `e` (matching RFC 3447)

JSON Web Algorithms (JWA)

- Normative changes made:
  - Merged `enc`, `int`, and `kdf` into single `enc` header parameter
  - Defined composite algorithms `A128CBC+HS256` and `A256CBC+HS512`
  - Added additional input values to KDF calculations: output length, AlgID, PartyUInfo, PartyVInfo
  - Changed RSA key parameter names `mod` and `exp` to `n` and `e` (matching RFC 3447)