JOSE Open Issues on Existing Features and Document Structuring Issues

Mike Jones
Microsoft Identity Standards Architect
March 27, 2012

Clarify `typ` Header Parameter

- Clarify the intended use of the `typ` Header Parameter across the JWS, JWE, and JWT specifications
  - Recommendation: State intended use to convey data type information about payload/plaintext
- Decide whether a registry of `typ` values is appropriate
  - Recommendation: Create Registry

Clarify Key ID (`kid`) Semantics

- What happens if a `kid` header is received with an unrecognized value? Is that an error? Should it be treated as if it's empty?
  - Recommendation: Treat as error

Combine the JWS and JWE alg parameter registries?

- Combine the JWS and JWE alg parameter registries?
  - Recommendation: Yes – in JWA spec
- Combine the header parameter registries?
  - Recommendation: No – Other than alg, these parameters are mostly quite different

Should the JWE Encrypted Key be moved to the header?

- Should the JWE Encrypted Key be moved to the header or left in a separate period-separated part to prevent double base64 encoding?
- JWE would have 3 parts like JWS, instead of 4
- Doing this would add about 20 bytes to every JWE
  - Recommendation: Leave as-is

Should JWK `alg` family definitions "`EC`" and "`RSA`" be moved to JWA?

- Would result in all the family-specific parameter definitions also moving there ("`crv`", "`x`", "`y`", "`mod`", "`exp`"), leaving almost no normative text in the JWK spec
- Seems like it would significantly reduce spec readability and so was not done
  - Recommendation: Leave as-is

Consider how additional key families would be added to JWK

- At present, would happen by revising spec
- Alternatively, new key families could be added to JWA
  - Recommendation: No change needed – either method is acceptable