JOSE New Specs & New Features

Mike Jones
Microsoft Identity Standards Architect
March 27, 2012

New Features

- JWS and JWE:
  - `jpk` for including JWK public key in header
  - `x5c` for including X.509 certificate chain in header
- JWE:
  - Add integrity check for non-AEAD algorithms
- JWA:
  - Add AES Key Wrap with 512 bit keys (`A512KW`)
  - Moved JWS `"alg":"none"` here from JWT spec

New JSON Serialization Specs

- Meet WG requirements:
  - JSON top-level representations of signed/HMACed and encrypted content
  - Multiple signatures/HMACs over same payload
  - Encrypt same plaintext to multiple recipients
- New Specs:
  - JSON Web Signature JSON Serialization (JWS-JS)
    - draft-jones-json-web-signature-json-serialization
  - JSON Web Encryption JSON Serialization (JWE-JS)
    - draft-jones-json-web-encryption-json-serialization

Example JWS-JS


```
{"headers":[
   "eyJhbGciOiJSUzI1NiJ9",
   "eyJhbGciOiJFUzI1NiJ9"],
 "payload":"eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0
    dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ",
 "signatures":[
   "cC4hiUPoj9Eetdgtv3hF80EGrhuB__dzERat0XF9g2VtQgr9PJbu3XOiZj5RZ
    mh7AAuHIm4Bh-0Qc_lF5YKt_O8W2Fp5jujGbds9uJdbF9CUAr7t1dnZcAcQjbKBY
    NX4BAynRFdiuB--f_nZLgrnbyTyWzO75vRK5h6xBArLIARNPvkSjtQBMHlb1L07Q
    e7K0GarZRmB_eSN9383LcOLn6_dO--xi12jzDwusC-eOkHWEsqtFZESc6BfI7noO
    PqvhJ1phCnvWh6IeYI2w9QOYEUipUTI8np6LbgGY9Fs98rqVt5AXLIhWkWywlVmt
    VrBp0igcN_IoypGlUPQGe77Rw",
   "DtEhU3ljbEg8L38VWAfUAqOyKAM6-Xx-F4GawxaepmXFCgfTjDxw5djxLa8IS
    lSApmWQxfKTUJqPP3-Kg6NU1Q"]
}
```

Compare to JWS Example

Format *Header.Payload.Signature*:

```
eyJhbGciOiJFUzI1NiJ9.
eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0
dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ.
lSApmWQxfKTUJqPP3-Kg6NU1Q
```

Why are the headers base64url encoded?

- Why:
  - `"eyJhbGciOiJFUzI1NiJ9"`
- Rather than:
  - `{"alg":"ES256"}`

- Simple answer:
  - Header contents is signed/HMACed

Request for WG Draft Status

- Request WG decision to move JSON Serialization docs to WG doc status
  - JSON Web Signature JSON Serialization (JWS-JS)
    - draft-jones-json-web-signature-json-serialization
  - JSON Web Encryption JSON Serialization (JWE-JS)
    - draft-jones-json-web-encryption-json-serialization