JSON Private and Symmetric Key

draft-jones-jose-json-private-and-symmetric-key

Mike Jones

March 13, 2013

IETF 86

Overview

- JSON representation for private and symmetric keys
  - Symmetric keys added since IETF 85 per WG request
- Complements JWK public key representations
  - Written as an extension to JWK
- *Created in response to interest by W3C WebCrypto WG*
- *Also created to meet needs of XMPP use case*

Elliptic Curve Private Key Example


```
{"alg":"EC",
 "crv":"P-256",
 "x":"MKBCTNIcKUSDii11ySs3526iDZ8AiTo7Tu6KPAqv7D4",
 "y":"4Etl6SRW2YiLUrN5vfvVHuhp7x8PxltmWWlbbM4IFyM",
 "d":"870MB6gfuTJ4HtUnUvYMyJpr5eUZNP4Bk43bVdj3eAE",
 "use":"enc",
 "kid":"1"
}
```

RSA Private Key Example


```
{"alg":"RSA",
 "n":"0vx7agoebGcQSuuPiLJXZptN9nndrQmbXEps2aiAFbWhM78LhWx4cbbfAAtVT86zwu1RK7aPFFxuhDR1L6tS
   oc_BJECPebWKRXjBZCiFV4n3oknjhMstn64tZ_2W-5JsGY4Hc5n9yBXArwl93lqt7_RN5w6Cf0h4QyQ5v-65YGj
   QR0_FDW2QvzqY368QQMicAtaSqzs8KJZgnYb9c7d0zgdAZHzu6qMQvRL5hajrn1n91CbOpbISD08qNLyrdkt-bF
   TWhAI4vMQFh6WeZu0fM4lFd2NcRwr3XPksINHaQ-G_xBniIqbw0Ls1jF44-csFCur-kEgU8awapJzKnqDKgw",
 "e":"AQAB",
 "d":"X4cTteJY_gn4FYPsXB8rdXix5vwsg1FLN5E3EaG6RJoVH-HLLKD9M7dx5oo7GURknchnrRweUkC7hT5fJLM0
   WbFAKNLWY2vv7B6NqXSzUvxT0_YSfqijwp3RTzlBaCxWp4doFk5N2o8Gy_nHNKroADIkJ46pRUohsXywbReAdYa
   MwFs9tv8d_cPVY3i07a3t8MN6TNwm0dSawm9v47UiCl3Sk5ZiG7xojPLu4sbg1U2jx4IBTNBznbJSzFHK66jT8b
   gkuqsk0GjskDJk19Z4qwjwbsnn4j2WBii3RL-Us2lGVkY8fkFzme1z0HbIkfz0Y6mqnOYtqc0X4jfcKoAC8Q",
 "p":"83i-7IvMGXoMXCskv73TKr8637FiO7Z27zv8oj6pbWUQyLPQBQxtPVnwD20R-60eTDmD2ujnMt5PoqMrm8Rf
   mNhVWDtjjMmCMjOpSXicFHj7XOuVIYQyqVWlWEh6dN36GVZYk93N8Bc9vY41xy8B9RzzOGVQzXvNEvn7O0nVbfs",
 "q":"3dfOR9cuYq-0S-mkFLzgItgMEfFzB2q3hWehMuG0oCuqnb3vobLyumqjVZQO1dIrdwgTnCdpYzBcOfW5r370
   AFXjiWft_NGEiovonizhKpo9VVS78TzFgxkIdrecRezsZ-1kYd_s1qDbxtkDEgfAITAG9LUnADun4vIcb6yelxk",
 "dp":"G4sPXkc6Ya9y8oJW9_ILj4xuppu0lzi_H7VTkS8xj5SdX3coE0oimYwxIi2emTAue0UOa5dpgFGyBJ4c8tQ
   2VF402XRugKDTP8akYhFo5tAA77Qe_NmtuYZc3C3m3I24G2GvR5sSDxUyAN2zq8Lfn9EUms6rY3Ob8YeiKkTiBj0",
 "dq":"s9lAH9fggBsoFR8Oac2R_E2gw282rT2kGOAhvIllETE1efrA6huUUvMfBcMpn8lqeW6vzznYY5SSQF7pMdC
   _agI3nG8Ibp1BUb0JUiraRNqUfLhcQb_d9GF4Dh7e74WbRsobRonujTYN1xCaP6TO61jvWrX-L18txXw494Q_cgk",
 "qi":"GyM_p6JrXySiz1toFgKbWV-JdI3jQ4ypu9rbMWx3rQJBfmt0FoYzgUIZEVFEcOqwemRN81zoDAaa-Bk0KWN
   GDjJHZDdDmFhW3AN7lI-puxk_mHZGJ11rxyR8O55XLSe3SPmRfKwZI6yU24ZxvQKFYItdldUKGzO6Ia6zTKhAVRU",
 "kid":"2011-04-29"
}
```

Symmetric Key Example


```
{"kty":"oct",
 "alg":"A128KW",
 "k":"GawgguFyGrWKav7AX4VKUg"
}
```

Request for WG Action

- Request WG decision to:
  - Adopt spec as WG draft
    - (once rechartering is complete)

- Related decision:
  - Should this spec be folded into JWK & JWA specs?
  - The charter will allow us to, or to keep it separate