WebAuthn Working Group M. Jones
Internet-Draft Microsoft
Intended status: Informational May 30, 2018
Expires: December 1, 2018

# Using secp256k1 with JOSE and COSE
# draft-jones-webauthn-secp256k1-00

## Abstract

This specification defines algorithm encodings and representations enabling the Standards for Efficient Cryptography Group (SECG) elliptic curve "secp256k1" to be used for JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) messages.

## Status of This Memo

This Internet-Draft will expire on December 1, 2018.

## Copyright Notice

Table of Contents

## 1. Introduction

This specification defines algorithm encodings and representations enabling the Standards for Efficient Cryptography Group (SECG) elliptic curve "secp256k1" [SEC2] to be used for JSON Object Signing and Encryption (JOSE) [RFC7515] and CBOR Object Signing and Encryption (COSE) [RFC8152] messages.  The elliptic curve and associated algorithm are registered in appropriate IANA JOSE and COSE registries.

### 1.1. Requirements Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 2. JOSE and COSE secp256k1 Curve Key Representations

The Standards for Efficient Cryptography Group (SECG) elliptic curve "secp256k1" [SEC2] is represented in a JSON Web Key (JWK) [RFC7517] using these values:

- "kty": "EC"
- "crv": "P-256K"

plus "x" and "y" values to represent the curve point for the key. Other optional values such as "alg" MAY also be present.

It is represented in a COSE_Key [RFC8152] using these values:

- "kty" (1): "EC2" (2)
- "crv" (-1): "P-256K" (TBD - requested assignment 8)

plus "x" (-2) and "y" (-3) values to represent the curve point for the key.  Other optional values such as "alg" (3) MAY also be present.

## 3. ECDSA Signature with secp256k1 Curve

The ECDSA signature algorithm is defined in [DSS].  Implementations need to check that the key type is "EC" for JOSE or "EC2" (2) for COSE when creating or verifying a signature.

The ECDSA algorithm specified in this document is:

| JOSE Alg Name | COSE Alg Value | Description |
|---|---|---|
| ES256K | TBD (requested assignment -43) | ECDSA w/ secp256k1 Curve |

Table 1: ECDSA Algorithm Values

## 4. IANA Considerations

### 4.1. JSON Web Key Elliptic Curve Registration

This section registers the following value in the IANA "JSON Web Key Elliptic Curve" registry [IANA.JOSE.Curves].

- Curve Name: P-256K
- Curve Description: SECG secp256k1 Curve
- JOSE Implementation Requirements: Optional
- Change Controller: IESG
- Specification Document(s): Section 2 of [[ this specification ]]

### 4.2. JOSE Algorithm Registration

This section registers the following value in the IANA "JSON Web Signature and Encryption Algorithms" registry [IANA.JOSE.Algorithms].

- Algorithm Name: ES256K
- Algorithm Description: ECDSA w/ secp256k1 Curve
- Algorithm Usage Locations: alg

- JOSE Implementation Requirements: Optional
- Change Controller: IESG
- Reference: Section 3 of [[ this specification ]]
- Algorithm Analysis Document(s): [SEC2]

### 4.3. COSE Elliptic Curves Registration

This section registers the following value in the IANA "COSE Elliptic Curves" registry [IANA.COSE.Curves].

- Name: P-256K
- Value: TBD (requested assignment 8)
- Key Type: EC2
- Description: SECG secp256k1 Curve
- Change Controller: IESG
- Reference: Section 2 of [[ this specification ]]
- Recommended: Yes

### 4.4. COSE Algorithm Registration

This section registers the following value in the IANA "COSE Algorithms" registry [IANA.COSE.Algorithms].

- Name: ES256K
- Value: TBD (requested assignment -43)
- Description: ECDSA w/ secp256k1 Curve
- Reference: Section 3 of this document
- Recommended: Yes

## 5. Security Considerations

Care should be taken that a secp256k1 key not be mistaken for a P-256 key, given that their representations are the same except for the "crv" value.

The procedures and security considerations described in the [SEC1], [SEC2], and [DSS] specifications apply to implementations of this specification.

## 6. References

### 6.1. Normative References

[DSS]      National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)", FIPS PUB 186-4, July 2013, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[SEC1] Standards for Efficient Cryptography Group, "SEC 1: Elliptic Curve Cryptography", Version 2.0, May 2009, <http://www.secg.org/sec1-v2.pdf>.

[SEC2] Standards for Efficient Cryptography Group, "SEC 2: Recommended Elliptic Curve Domain Parameters", Version 2.0, January 2010, <http://www.secg.org/sec2-v2.pdf>.

### 6.2. Informative References

[IANA.COSE.Algorithms] IANA, "COSE Algorithms", <https://www.iana.org/assignments/cose/cose.xhtml#algorithms>.

[IANA.COSE.Curves] IANA, "COSE Elliptic Curves", <https://www.iana.org/assignments/cose/cose.xhtml#elliptic-curves>.

[IANA.JOSE.Algorithms] IANA, "JSON Web Signature and Encryption Algorithms", <https://www.iana.org/assignments/jose/jose.xhtml#web-signature-encryption-algorithms>.

[IANA.JOSE.Curves]
IANA, "JSON Web Key Elliptic Curve", <https://www.iana.org/assignments/jose/jose.xhtml#web-key-elliptic-curve>.

## Acknowledgements

TBD

## Document History

[[ to be removed by the RFC Editor before publication as an RFC ]]

-00

- Initial version.

## Author's Address

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: http://self-issued.info/