COSE and JOSE Registrations for WebAuthn Algorithms

draft-ietf-cose-webauthn-algorithms-01

Abstract

The W3C Web Authentication (WebAuthn) specification and the FIDO2 Client to Authenticator Protocol (CTAP) specification use COSE algorithm identifiers. This specification registers algorithms in the IANA "COSE Algorithms" registry that are used by WebAuthn and CTAP implementations that are not already registered. Also, they are registered in the IANA "JSON Web Signature and Encryption Algorithms" registry, when not already registered there.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

This specification defines how to use several algorithms with COSE [RFC8152] that are used by implementations of the W3C Web Authentication (WebAuthn) [WebAuthn] and FIDO2 Client to Authenticator Protocol (CTAP) [CTAP] specifications. These algorithms are registered in the IANA "COSE Algorithms" registry [IANA.COSE.Algorithms] and also in the IANA "JSON Web Signature and Encryption Algorithms" registry [IANA.JOSE.Algorithms], when not already registered there.

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. RSASSA-PKCS1-v1_5 Signature Algorithm

The RSASSA-PKCS1-v1_5 signature algorithm is defined in [RFC8017]. The RSASSA-PKCS1-v1_5 signature algorithm is parameterized with a hash function \((h)\).

A key of size 2048 bits or larger MUST be used with these algorithms. Implementations need to check that the key type is 'RSA' when creating or verifying a signature.

The RSASSA-PKCS1-v1_5 algorithms specified in this document are in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Hash</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS256</td>
<td>TBD (temporary assignment -257 already in place)</td>
<td>SHA-256</td>
<td>RSASSA-PKCS1-v1_5 using SHA-256</td>
</tr>
<tr>
<td>RS384</td>
<td>TBD (temporary assignment -258 already in place)</td>
<td>SHA-384</td>
<td>RSASSA-PKCS1-v1_5 using SHA-384</td>
</tr>
<tr>
<td>RS512</td>
<td>TBD (temporary assignment -259 already in place)</td>
<td>SHA-512</td>
<td>RSASSA-PKCS1-v1_5 using SHA-512</td>
</tr>
<tr>
<td>RS1</td>
<td>TBD (temporary assignment -65535 already in place)</td>
<td>SHA-1</td>
<td>RSASSA-PKCS1-v1_5 using SHA-1</td>
</tr>
</tbody>
</table>

Table 1: RSASSA-PKCS1-v1_5 Algorithm Values

3. Using secp256k1 with JOSE and COSE

This section 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.

3.1. 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": "secp256k1"

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): "secp256k1" (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.

### 3.2. ECDSA Signature with secp256k1 Curve

The ECDSA signature algorithm is defined in [DSS]. This specification defines the use of ECDSA with the secp256k1 curve and the SHA-256 [DSS] cryptographic hash function. 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 secp256k1 SHA-256 digital signature is generated as follows:

1. Generate a digital signature of the JWS Signing Input or the COSE payload using ECDSA secp256k1 SHA-256 with the desired private key. The output will be the pair (R, S), where R and S are 256-bit unsigned integers.

2. Turn R and S into octet sequences in big-endian order, with each array being be 32 octets long. The octet sequence representations MUST NOT be shortened to omit any leading zero octets contained in the values.

3. Concatenate the two octet sequences in the order R and then S. (Note that many ECDSA implementations will directly produce this concatenation as their output.)

4. The resulting 64-octet sequence is the JWS Signature or COSE signature value.

The ECDSA secp256k1 SHA-256 algorithm specified in this document uses these identifiers:
<table>
<thead>
<tr>
<th>JOSE Alg Name</th>
<th>COSE Alg Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES256K</td>
<td>TBD (requested assignment -43)</td>
<td>ECDSA using secp256k1 curve and SHA-256</td>
</tr>
</tbody>
</table>

Table 2: ECDSA Algorithm Values

4. IANA Considerations

4.1. COSE Algorithms Registrations

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

- Name: RS256
  - Value: TBD (temporary assignment -257 already in place)
  - Description: RSASSA-PKCS1-v1_5 using SHA-256
  - Reference: Section 2 of this document
  - Recommended: No

- Name: RS384
  - Value: TBD (temporary assignment -258 already in place)
  - Description: RSASSA-PKCS1-v1_5 using SHA-384
  - Reference: Section 2 of this document
  - Recommended: No

- Name: RS512
  - Value: TBD (temporary assignment -259 already in place)
  - Description: RSASSA-PKCS1-v1_5 using SHA-512
  - Reference: Section 2 of this document
  - Recommended: No

- Name: RS1
  - Value: TBD (temporary assignment -65535 already in place)
  - Description: RSASSA-PKCS1-v1_5 using SHA-1
  - Reference: Section 2 of this document
  - Recommended: Deprecated

- Name: ES256K
  - Value: TBD (requested assignment -43)
  - Description: ECDSA using secp256k1 curve and SHA-256
  - Reference: Section 3.2 of this document
  - Recommended: Yes
4.2. COSE Elliptic Curves Registrations

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

- Name: secp256k1
- Value: TBD (requested assignment 8)
- Key Type: EC2
- Description: SECG secp256k1 curve
- Change Controller: IESG
- Reference: Section 3.1 of [[ this specification ]]
- Recommended: Yes

4.3. JOSE Algorithms Registrations

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 using secp256k1 curve and SHA-256
- Algorithm Usage Locations: alg
- JOSE Implementation Requirements: Optional
- Change Controller: IESG
- Reference: Section 3.2 of [[ this specification ]]
- Algorithm Analysis Document(s): [SEC2]

4.4. JSON Web Key Elliptic Curves Registrations

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

- Curve Name: secp256k1
- Curve Description: SECG secp256k1 curve
- JOSE Implementation Requirements: Optional
- Change Controller: IESG
- Specification Document(s): Section 3.1 of [[ this specification ]]

5. Security Considerations

5.1. RSA Key Size Security Considerations

The security considerations on key sizes for RSA algorithms from Section 6.1 of [RFC8230] also apply to the RSA algorithms in this specification.
5.2. RSASSA-PKCS1-v1_5 with SHA-2 Security Considerations

The security considerations on the use of RSASSA-PKCS1-v1_5 with SHA-2 hash functions from Section 8.3 of [RFC7518] also apply to their use in this specification. For that reason, these algorithms are registered as being "Not Recommended".

5.3. RSASSA-PKCS1-v1_5 with SHA-1 Security Considerations

The security considerations on the use of the SHA-1 hash function from [RFC6194] apply in this specification. For that reason, the "RS1" algorithm is registered as "Deprecated". It MUST NOT be used by COSE implementations.

A COSE algorithm identifier for this algorithm is nonetheless being registered because deployed TPMs continue to use it, and therefore WebAuthn implementations need a COSE algorithm identifier for "RS1" when TPM attestations using this algorithm are being represented.

5.4. secp256k1 Security Considerations

Care should be taken that a secp256k1 key is not 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


6.2. Informative References


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


Acknowledgements

Thanks to Stephen Farrell, John Fontana, Jeff Hodges, John Mattsson, Tony Nadalin, Matt Palmer, Jim Schaad, Goeran Selander, Wendy Seltzer, Sean Turner, and Samuel Weiler for their roles in registering these algorithm identifiers.

Document History

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

-01
Internet-DraCOSE and JOSE Registrations for WebAuthn Algorithm  July 2019

- Changed the JOSE curve identifier from "P-256K" to "secp256k1".
- Specified that secp256k1 signing is done using the SHA-256 hash function.
- Created the initial working group draft from draft-jones-cose-additional-algorithms-00, changing only the title, date, and history entry.

Author’s Address

Michael B. Jones
Microsoft

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