Workgroup: WebAuthn Working Group
Internet-Draft: draft-dang-webauthn-sm2-00
Published: 6 November 2021
Intended Status: Informational
Expires: 10 May 2022
Authors: F. Dang
Tsinghua University

Using SM2 with JOSE and COSE

Abstract

This specification defines algorithm encodings and representations enabling the ISO/IEC 14888-3:2018 elliptic curve "SM2" 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 10 May 2022.

Copyright Notice

Table of Contents

1. Introduction
  1.1. Requirements Notation and Conventions
2. JOSE and COSE SM2 Curve Key Representations
3. ECDSA Signature with SM2 Curve
4. IANA Considerations
  4.1. JSON Web Key Elliptic Curve Registration
  4.2. JOSE Algorithm Registration
  4.3. COSE Elliptic Curves Registration
  4.4. COSE Algorithm Registration
5. Security Considerations
6. References
  6.1. Normative References
  6.2. Informative References
Appendix A. Document History
Author's Address

1. Introduction

This specification defines algorithm encodings and representations enabling the ISO/IEC 14888-3:2018 elliptic curve "SM2" [ISO14888-3] 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 SM2 Curve Key Representations

The ISO/IEC 14888-3:2018 elliptic curve "SM2" [ISO14888-3] is represented in a JSON Web Key (JWK) [RFC7517] using these values:

*kty: EC
*crv: SM2

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): SM2 (TBD - requested assignment 9)

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 SM2 Curve

The ECDSA signature algorithm is defined in [ISO14888-3]. 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
SM2	TBD (requested assignment -48)	ECDSA w/ SM2 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: curveSM2
*Curve Description: SM2 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: SM2
*Algorithm Description: ECDSA w/ SM2 Curve
*Algorithm Usage Locations: alg
*JOSE Implementation Requirements: Optional
*Change Controller: IESG
*Reference: Section 3 of [[this specification]]
*Algorithm Analysis Document(s): [ISO14888-3]

4.3. COSE Elliptic Curves Registration

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

*Name: curveSM2
*Value: TBD (requested assignment 9)

*Key Type: EC2
*Description: SM2 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: SM2
*Value: TBD (requested assignment -48)
*Description: ECDSA w/ SM2 Curve
*Reference: Section 3 of this document
*Recommended: Yes

5. Security Considerations

The procedures and security considerations described in the [ISO14888-3] specifications apply to implementations of this specification.

6. References

6.1. Normative References

[ISO14888-3] International Organization for Standardization, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", November 2018.

[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>.

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>.

Appendix A. Document History

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

-00

*Initial version.

Author's Address

Fan Dang
Tsinghua University
Beijing
100084

China

Email: dangfan@tsinghua.edu.cn