

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 2, 2021

K. Den Hartog, Ed.
Mattr
May 31, 2021

Pairing Friendly Curves representations in JOSE and COSE
draft-denhartog-pairing-curves-jose-cose-00

Abstract

This specification defines representations enabling the Standards for Pairing Friendly Curves 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 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 December 2, 2021.

Copyright Notice

Copyright (c) 2021 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 the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
1.1. Notational Conventions	3
2. Barreto Naehrig (BN) Curves	3
2.1. BN256 Curve	3
2.1.1. Bn256G1 Curve JOSE Key Representation	3
2.1.2. Bn256G1 Curve COSE Key Representation	3
2.1.3. Bn256G2 Curve JOSE Key Representation	3
2.1.4. Bn256G2 Curve COSE Key Representation	4
2.2. BN462 Curve	4
2.2.1. Bn462G1 Curve JOSE Key Representation	4
2.2.2. Bn462G1 Curve COSE Key Representation	4
2.2.3. Bn462G2 Curve JOSE Key Representation	4
2.2.4. Bn462G2 Curve COSE Key Representation	5
3. Barreto Lynn Scott (BLS) Curves	5
3.1. BLS12-381 Curve	5
3.1.1. Bls12381G1 Curve JOSE Key Representation	5
3.1.2. Bls12381G1 Curve COSE Key Representation	5
3.1.3. Bls12381G2 Curve JOSE Key Representation	5
3.1.4. Bls12381G2 Curve COSE Key Representation	6
3.2. BLS48-581 Curve	6
3.2.1. Bls48581G1 Curve JOSE Key Representation	6
3.2.2. Bls48581G1 Curve COSE Key Representation	6
3.2.3. Bls48581G2 Curve JOSE Key Representation	6
3.2.4. Bls48581G2 Curve COSE Key Representation	7
4. IANA Considerations	7
4.1. JSON Web Key Elliptic Curve Registrations	7
4.2. COSE Elliptic Curve Registrations	8
5. Security Considerations	10
6. Privacy Considerations	10
7. Acknowledgements	10
8. Normative References	11
Author's Address	11

1. Introduction

This specification defines algorithm encodings and representations enabling the Standard Pairing Friendly Curves to be used for JSON Object Signing and Encryption (JOSE) [RFC7517] [RFC7517] and CBOR Object Signing and Encryption (COSE) [RFC8152] [RFC8152] messages. The elliptic curve and associated algorithm are registered in appropriate IANA JOSE and COSE registries.

1.1. Notational 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 RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Barreto Naehrig (BN) Curves

2.1. BN256 Curve

2.1.1. Bn256G1 Curve JOSE Key Representation

The pairing friendly elliptic curve "BN256" which uses the largest prime-order subgroup of $E(\text{GF}(p))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values: o "kty": "OKP" o "crv": "Bn256G1" plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using [SEC1] [SEC1] format and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

2.1.2. Bn256G1 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bn256G1" (TBD - requested assignment 9)

plus "x" (-2) values to represent the curve point for the key. The "x" value MUST be encoded using [SEC1] [SEC1] point compression format.

2.1.3. Bn256G2 Curve JOSE Key Representation

The pairing friendly elliptic curve "BN256" which uses an r-order subgroup of $E'(\text{GF}(p^2))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values:

- o "kty": "OKP"
- o "crv": "Bn256G2"

plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using [SEC1] [SEC1] and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

2.1.4. Bn256G2 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bn256G2" (TBD - requested assignment 10)

plus "x" (-2) values to represent the curve point for the key. The "x" value MUST be encoded using [SEC1] [SEC1] point compression format.

2.2. BN462 Curve

2.2.1. Bn462G1 Curve JOSE Key Representation

The pairing friendly elliptic curve "BN462" which uses the largest prime-order subgroup of $E(\text{GF}(p))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values:

- o "kty": "OKP"
- o "crv": "Bn462G1"

plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using [SEC1] [SEC1] and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

2.2.2. Bn462G1 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bn462G1" (TBD - requested assignment 11)

plus "x" (-2) values to represent the curve point for the key.

2.2.3. Bn462G2 Curve JOSE Key Representation

The pairing friendly elliptic curve "BN462" which uses an r-order subgroup of $E'(\text{GF}(p^2))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values:

- o "kty": "OKP"
- o "crv": "Bn462G2"

plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using [SEC1] [SEC1] and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

2.2.4. Bn462G2 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bn462G2" (TBD - requested assignment 12)

plus "x" (-2) values to represent the curve point for the key.

3. Barreto Lynn Scott (BLS) Curves

3.1. BLS12-381 Curve

3.1.1. Bls12381G1 Curve JOSE Key Representation

The pairing friendly elliptic curve "BLS12-381" which uses the largest prime-order subgroup of $E(\text{GF}(p))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values:

- o "kty": "OKP"
- o "crv": "Bls12381G1"

plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using the Z-Cash serialization defined in [DPFC09] [DPFC09] and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

3.1.2. Bls12381G1 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bls12381G1" (TBD - requested assignment 13)

plus "x" (-2) values to represent the curve point for the key.

3.1.3. Bls12381G2 Curve JOSE Key Representation

The pairing friendly elliptic curve "BLS12-381" which uses an r-order subgroup of $E'(\text{GF}(p^2))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values:

- o "kty": "OKP"
- o "crv": "Bls12381G2"

plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using the Z-Cash serialization defined in [DPFC09] [DPFC09] and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

3.1.4. Bls12381G2 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bls12381G2" (TBD - requested assignment 14)

plus "x" (-2) values to represent the curve point for the key.

3.2. BLS48-581 Curve

3.2.1. Bls48581G1 Curve JOSE Key Representation

The pairing friendly elliptic curve "BLS48-581" which uses the largest prime-order subgroup of $E(\text{GF}(p))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values:

- o "kty": "OKP"
- o "crv": "Bls48581G1"

plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using [SEC1] [SEC1] and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

3.2.2. Bls48581G1 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bls48581G1" (TBD - requested assignment 15)

plus "x" (-2) values to represent the curve point for the key.

3.2.3. Bls48581G2 Curve JOSE Key Representation

The pairing friendly elliptic curve "BLS48-581" which uses the largest prime-order subgroup of $E'(\text{GF}(p^8))$ is represented in a JSON Web Key (JWK) [RFC7517] [RFC7517] using these values:

- o "kty": "OKP"
- o "crv": "Bls48581G2"

plus "x" value to represent the curve point for the public key. The "x" value MUST be encoded using [SEC1] [SEC1] and MUST be base64url encoded without padding as defined in [RFC7515] [RFC7515] Appendix C.

3.2.4. Bls48581G2 Curve COSE Key Representation

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

- o "kty" (1): "OKP" (1)
- o "crv" (-1): "Bls48581G1" (TBD - requested assignment 16)

plus "x" (-2) values to represent the curve point for the key.

4. IANA Considerations

4.1. JSON Web Key Elliptic Curve Registrations

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

- o Curve Name: Bn256G1
- o Curve Description: 256 bit Barreto-Naehrig pairing friendly curve using the largest prime-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Prohibited
- o Change Controller: IESG
- o Specification Document(s): Section 2.1 of [[this specification]]

- o Curve Name: Bn256G2
- o Curve Description: 256 bit Barreto-Naehrig pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^2))$
- o JOSE Implementation Requirements: Prohibited
- o Change Controller: IESG
- o Specification Document(s): Section 2.3 of [[this specification]]

- o Curve Name: Bn462G1
- o Curve Description: 462 bit Barreto-Naehrig pairing friendly curve using the largest prime-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 2.5 of [[this specification]]

- o Curve Name: Bn462G2
- o Curve Description: 462 bit Barreto-Naehrig pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^2))$

- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 2.7 of [[this specification]]
- o Curve Name: Bls12381G1
- o Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.1 of [[this specification]]
- o Curve Name: Bls12381G2
- o Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^2))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.3 of [[this specification]]
- o Curve Name: Bls48581G1
- o Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.5 of [[this specification]]
- o Curve Name: Bls48581G1
- o Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^8))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.7 of [[this specification]]

4.2. COSE Elliptic Curve Registrations

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

- o Curve Name: Bn256G1
- o Value: TBD (requested assignment 9)
- o Key Type: OKP
- o Curve Description: 256 bit Barreto-Naehrig pairing friendly curve using the largest prime-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Prohibited
- o Change Controller: IESG

- o Specification Document(s): Section 2.2 of [[this specification]]
- o Recommended: No (Prohibited)

- o Curve Name: Bn256G2
- o Value: TBD (requested assignment 10)
- o Key Type: OKP
- o Curve Description: 256 bit Barreto-Naehrig pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^2))$
- o JOSE Implementation Requirements: Prohibited
- o Change Controller: IESG
- o Specification Document(s): Section 2.4 of [[this specification]]
- o Recommended: No (Prohibited)

- o Curve Name: Bn462G1
- o Value: TBD (requested assignment 11)
- o Key Type: OKP
- o Curve Description: 462 bit Barreto-Naehrig pairing friendly curve using the largest prime-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 2.6 of [[this specification]]
- o Recommended: No

- o Curve Name: Bn462G2
- o Value: TBD (requested assignment 12)
- o Key Type: OKP
- o Curve Description: 462 bit Barreto-Naehrig pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^2))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 2.8 of [[this specification]]
- o Recommended: No

- o Curve Name: Bls12381G1
- o Value: TBD (requested assignment 13)
- o Key Type: OKP
- o Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.2 of [[this specification]]
- o Recommended: Yes

- o Curve Name: Bls12381G2
- o Value: TBD (requested assignment 14)
- o Key Type: OKP

- o Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^2))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.4 of [[this specification]]
- o Recommended: Yes

- o Curve Name: Bls48581G1
- o Value: TBD (requested assignment 15)
- o Key Type: OKP
- o Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E(\text{GF}(p))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.6 of [[this specification]]
- o Recommended: No

- o Curve Name: Bls48581G1
- o Value: TBD (requested assignment 16)
- o Key Type: OKP
- o Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing friendly curve using an r-order subgroup of $E'(\text{GF}(p^8))$
- o JOSE Implementation Requirements: Optional
- o Change Controller: IESG
- o Specification Document(s): Section 3.8 of [[this specification]]
- o Recommended: No

5. Security Considerations

See [DPFC09] [DPFC09] for additional details about security considerations of the curves used. Implementers should also consider section 9 of [RFC7517] [RFC7517] when implementing this work.

6. Privacy Considerations

To be added.

7. Acknowledgements

The authors of this draft would like to acknowledge the following individuals for the significant contribution of ideas and time spent reviewing this document:

8. Normative References

- [DPFC09] IRTF CFRG, "Pairing-Friendly Curves", November 2020, <<https://tools.ietf.org/html/draft-irtf-cfrg-pairing-friendly-curves-09>>.
- [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 (SECG), "SEC 1: Elliptic Curve Cryptography", 2009, <<https://www.secg.org/sec1-v2.pdf>>.

Author's Address

Kyle Den Hartog (editor)
Mattr

Email: kyle.denhartog@mattr.global