Workgroup: COSE
Internet-Draft:
draft-ietf-cose-bls-key-representations-05
Published: 17 March 2024
Intended Status: Standards Track
Expires: 18 September 2024
Authors: T. Looker M. Jones
Mattr Self-Issued Consulting

Barreto-Lynn-Scott Elliptic Curve Key Representations for JOSE and COSE

Abstract

This specification defines how to represent cryptographic keys for the pairing-friendly elliptic curves known as Barreto-Lynn-Scott (BLS), for use with the key representation formats of JSON Web Key (JWK) and COSE (COSE_Key).

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/tplooker/draft-ietf-cose-bls-key-representations.

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 18 September 2024.

Copyright Notice

Table of Contents

1. Introduction

This specification defines how to represent cryptographic keys for the pairing-friendly elliptic curves known as Barreto-Lynn-Scott [BLS], for use with the key representation formats of JSON Web Key (JWK) and COSE_Key. This specification registers the elliptic curves in appropriate IANA JOSE and COSE registries.

There are a variety of applications for pairing based cryptography including schemes already published as RFCs, such as Identity-Based Cryptography [RFC5091] Sakai-Kasahara Key Encryption (SAKKE) [RFC6508], and Identity-Based Authenticated Key Exchange (IBAKE) [RFC6539]. SAKKE is applied to Multimedia Internet KEYing (MIKEY) via [RFC6509] and IBAKE is applied for a similar application via [RFC6267].

This branch of cryptography has also been used to develop privacy-preserving cryptographic hardware attestations schemes, including the Elliptic Curve Direct Anonymous Attestation (ECDAA) in the Trusted Platform Modules [TPM] specified by the Trusted Computing Group. Further work on similar schemes has also occurred at the FIDO Alliance [ECDAA]. Similarly, Intel released [EPID] which provides a solution to remote hardware attestation for Intel Software Guard Extension (SGX) enabled environments.

More recently, applications of pairing based cryptography using the Barreto-Lynn-Scott curves include the standardization effort for BLS Signatures [id.draft.bls-signature], which are used extensively in multiple blockchain projects due to their unique signature aggregation properties, including [Ethereum] [DFINITY] [Algorand]. Additionally, efforts are under way to standardize the general purpose short group signature scheme of BBS Signatures [BBS], which features novel properties such as multi-message signing and selective disclosure alongside zero knowledge proving. It is intended that this draft will help with these efforts by standardizing the associated cryptographic key representation in the popular formats of JWK and COSE_Key.

Other relevant work to this draft includes [JWP] which is extending the JOSE family of specifications to provide support for representing a variety of new proof based cryptographic schemes such as [BBS] which as referred to above uses the Barreto-Lynn-Scott curves.

There are multiple different pairing-friendly curves in active use; however, this draft focuses on a definition for the Barreto-Lynn-Scott curves due to them being the most "widely used" and "efficient" whilst achieving 128-bit and 256-bit security (BLS12-381 and BLS48-581 respectively).

More extensive discussion on the broader application of pairing based cryptography and the assessment of various elliptic curves (including the BLS family) can be found in [id.draft.pairing-friendly-curves].

2. Conventions and Definitions

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.

2.1. Point Coordinates Encoding

A point representing a public key will either be in the G1 or G2 subgroup of a curve. Depending on which one of the subgroups the public key will belong to, different serialization procedures need to

be used, to encode its coordinates. Most specifically, if the public key is a point in the G1 subgroup, each of its coordinates MUST be encoded using the serialization defined in Section 2.3.5 of [SEC1]. If the public key is a point in the G2 subgroup, each of its coordinates MUST be serialize using the procedure described in Appendix I.5 in [I-D.ietf-lwig-curve-representations].

2.2. Representation Definition

The following definitions apply to the pairing-friendly elliptic curves known as the Barreto-Lynn-Scott (BLS) curves.

2.2.1. JSON Web Key Representation

When expressing a cryptographic key for these curves in JSON Web Key (JWK) form, the following rules apply:

- The parameter "kty" MUST be present and set to "EC".
- The parameter "crv" MUST be present and value MUST be one defined in Section 2.2.3.
- The parameter "x" MUST be present whose value represents the x coordinate of the curve point for the public key. This value MUST be encoded using the procedure defined in Section 2.1 and MUST be base64url encoded without padding as defined in [RFC7515] Appendix C.
- The parameter "y" MUST be present whose value represents the y coordinate of the curve point for the public key. This value MUST be encoded using the procedure defined in Section 2.1 and MUST be base64url encoded without padding as defined in [RFC7515] Appendix C.
- The parameter "d" MUST be present for private key representations whose value MUST contain the little-endian representation of the private key base64url encoded without padding as defined in [RFC7515] Appendix C. This parameter MUST NOT be present for public keys.

2.2.2. COSE_Key Representation

When expressing a cryptographic key for these curves in COSE_Key form, the following rules apply:

- The parameter "kty" (1) MUST be present and set to "EC2" (2).
- The parameter "crv" (-1) MUST be present and value MUST be one defined in Section 2.2.3.
- The parameter "x" (-2) MUST be present whose value represents the x coordinate of the curve point for the public key. This value MUST be encoded using the procedure defined in Section 2.1 and MUST be base64url encoded without padding as defined in [RFC7515] Appendix C.

*The parameter "y" (-3) Must be present whose value represents the y coordinate of the curve point for the public key. This value MUST be encoded using the procedure defined in Section 2.1 and MUST be base64url encoded without padding as defined in [RFC7515] Appendix C.
*The parameter "d" (-4) MUST be present for private key representations whose value MUST contain the little-endian representation of the private key. This parameter MUST NOT be present for public keys.

2.2.3. Curve Parameter Registration

JWK "crv" value	COSE_Key "crv" value	Description
BLS12381G1	TBD (13 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding degree 12 with 381-bit p in the subgroup of G1 defined as E(GF(p)) of order r. The private key will be 32 bytes long. Each of the x and y coordinates of the public key will be 48 bytes long.
BLS12381G2	TBD (14 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding degree 12 with 381-bit p in the subgroup of G2 defined as E(GF(p^2)) of order r. The private key will be 32 bytes long. Each of the x and y coordinates of the public key will be 96 bytes long.
BLS48581G1	TBD (15 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding degree 48 with 581-bit p in the subgroup of G1 defined as E(GF(p)) of order r. The private key will be 65 bytes long. Each of the x and y coordinates of the public key will be 73 bytes long.
BLS48581G2	TBD (16 requested)	A cryptographic key on the Barreto-Lynn-Scott (BLS) curve featuring an embedding degree 48 with 581-bit p in the subgroup of G2 defined as E(GF(p^8)) of order r. The private key will be 65 bytes long. Each of the x and y coordinates of the public key will be 584 bytes long.

Table 1

3. Security Considerations

See [id.draft.pairing-friendly-curves] for additional details on security considerations for the curves used. Implementers should also

consider the general guidance provided in Section 9 of [RFC7517] and Section 17 of [RFC8152] when using this specification.

Furthermore, because this specification only defines the cryptographic key representations and not the usage of these keys with specific algorithms, implementers should be aware to follow any guidance that may be provided around appropriate usage of the keys and or additional steps that may be required to validate the keys within the context of particular algorithms.

4. IANA Considerations

4.1. JSON Web Key (JWK) Elliptic Curve Registrations

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

BLS12381G1

- *Curve Name: BLS12381G1
- *Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))
- *JOSE Implementation Requirements: Optional
- *Change Controller: IESG
- *Specification Document(s): Section 2.2.1

BLS12381G2

- *Curve Name: BLS12381G2
- *Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^2))
- *JOSE Implementation Requirements: Optional
- *Change Controller: IESG
- *Specification Document(s): Section 2.2.1

BLS48581G1

- *Curve Name: BLS48581G1
- *Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))
- *JOSE Implementation Requirements: Optional
- *Change Controller: IESG
- *Specification Document(s): Section 2.2.1

BLS48581G2

- *Curve Name: BLS48581G2

*Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^8))
*JOSE Implementation Requirements: Optional
*Change Controller: IESG
*Specification Document(s): Section 2.2.1

4.2. COSE Elliptic Curve Registrations

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

BLS12381G1

*Curve Name: BLS12381G1
*Value: TBD (13 requested)
*Key Type: EC2
*Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))
*JOSE Implementation Requirements: Optional
*Change Controller: IESG
*Specification Document(s): Section 2.2.2
*Recommended: Yes

BLS12381G2

*Curve Name: BLS12381G2
*Value: TBD (14 requested)
*Key Type: EC2
*Curve Description: 381 bit with an embedding degree of 12 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^2))
*JOSE Implementation Requirements: Optional
*Change Controller: IESG
*Specification Document(s): Section 2.2.2
*Recommended: Yes

BLS48581G1

*Curve Name: BLS48581G1
*Value: TBD (15 requested)
*Key Type: EC2
*Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E(GF(p))
*JOSE Implementation Requirements: Optional
*Change Controller: IESG
*Specification Document(s): Section 2.2.2
*Recommended: Yes

BLS48581G2

*Curve Name: BLS48581G2
*Value: TBD (16 requested)
*Key Type: EC2
*Curve Description: 581 bit with an embedding degree of 48 Barreto-Lynn-Scott pairing-friendly curve using the r-order subgroup of E'(GF(p^8))
*JOSE Implementation Requirements: Optional
*Change Controller: IESG
*Specification Document(s): Section 2.2.2
*Recommended: Yes

5. References

5.1. Normative References

[BLS] Barreto, P., Lynn, B., and M. Scott, "Constructing Elliptic Curves with Prescribed Embedding Degrees", 2003, <https://link.springer.com/chapter/10.1007/3-540-36413-7_19>.

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

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

[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>.

[id.draft.bls-signature] IETF CFRG, "BLS Signatures", 16 June 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-bls-signature-05>.

[id.draft.pairing-friendly-curves]
IETF CFRG, "Pairing-Friendly Curves", 10 May 2023, <https://www.ietf.org/archive/id/draft-irtf-cfrg-pairing-friendly-curves-11.html>.

5.2. Informative References

[BBS] IETF CFRG, "The BBS Signature Scheme", 21 December 2023, <https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-05.html>.

[ECDAA] FIDO Alliance, "ECDAA Algorithm", 2018, <https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-ecdaa-algorithm-v2.0-id-20180227.html>.

[EPID] Intel Corporation, "Intel (R) SGX: Intel (R) EPID Provisioning and Attestation Services", <https://software.intel.com/en-us/download/intel-sgx-intel-epid-provisioning-and-attestation-services>.

[I-D.ietf-lwig-curve-representations]
Struik, R., "Alternative Elliptic Curve Representations", Work in Progress, Internet-Draft, draft-ietf-lwig-curve-representations-23, 21 January 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-lwig-curve-representations-23>.

[JWP] Miller, J., Waite, D., and M. Jones, "JSON Web Proof", 21 October 2023, <https://www.ietf.org/archive/id/draft-ietf-jose-json-web-proof-02.html>.

[RFC5091] Boyen, X. and L. Martin, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, DOI 10.17487/RFC5091, December 2007, <https://www.rfc-editor.org/info/rfc5091>.

[RFC6267] Cakulev, V. and G. Sundaram, "MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)", RFC 6267, DOI 10.17487/RFC6267, June 2011, <https://www.rfc-editor.org/info/rfc6267>.

[RFC6508] Groves, M., "Sakai-Kasahara Key Encryption (SAKKE)", RFC 6508, DOI 10.17487/RFC6508, February 2012, <https://www.rfc-editor.org/info/rfc6508>.

[RFC6509] Groves, M., "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)", RFC 6509, DOI

10.17487/RFC6509, February 2012, <https://www.rfc-editor.org/info/rfc6509>.

[RFC6539] Cakulev, V., Sundaram, G., and I. Broustis, "IBAKE: Identity-Based Authenticated Key Exchange", RFC 6539, DOI 10.17487/RFC6539, March 2012, <https://www.rfc-editor.org/info/rfc6539>.

[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", 21 May 2009, <http://www.secg.org/sec1-v2.pdf>.

[TPM] Trusted Computing Group, "Trusted Platform Module", <https://trustedcomputinggroup.org/>.

Appendix A. JSON Web Key Examples

A.1. BLS12381 Key Pairs

The following examples showcase JWKs for both the G1 and G2 subgroups of the BLS12381 curve. Note, the examples also include the corresponding private key, expressed through the inclusion of the “d” parameter.

An example JWK for the BLS12381 curve where the public key is in the G1 subgroup.

```
{
  "kty": "EC",
  "crv": "BLS12381G1",
  "x": "Ed4GBGLVasEp4ejPz44CvllbTldfLLcm2QcIJluBL6p_SQmRrZvJNa3YaJ-Wx8Im
  "y": "AbdYAsAb20CHzlVW6VBO9i16BcGOmcYiMLlBEh9DfAiDu_1ZIAd1zewSi9f6517g
  "d": "3nc6_s38FVVlawbwmPFOjB4TlAPy_K2Tx39I7XnEnDc"
}
```

Another example of a different JWK for the BLS12381 curve where the public key is in the G1 subgroup.

```
{
  "kty": "EC",
  "crv": "BLS12381G1",
  "x": "EUGQExpzxebwmXEeqc39OI3J1NfUCMVQPqc_Lb-4dLu0xCaSrd0rDBMTFthd5r-2
  "y": "FNpXfp4a-5N7Cb528pwRhLINOmwyuhjKjPz8jcaxgCSNZCbjaYQsGoOhftRqWKpg
  "d": "OdNBrRDu89IrnlY5Hl-2CW-3cqW0Rw7IgQUuwLZ8gV4"
}
```


An example JWK for the BLS12381 curve where the public key is in the G2 subgroup.


```
{
  "kty": "EC",
  "crv": "BLS12381G2",
  "x": "Ajs8lstTgoTgXMF6QXdyh3m8k2ixxURGYLMaYylVK_x0F8HhE8zk0YWiGV3CHwpQ
Ea2sH4PBZLaYCn8se-1clmCORDsKxbbw3Js_Alu4OmkV9gmbJsy1YF2rt7Vxzs6S",
  "y": "BVkkrVEib-P_FMPHNtqxJymP3pV-H8fCdvPkoWInpFfM9tViyqD8JAmwDf64zU2h
BV_vvCQ632ScAooEExXuz1IeQH9D2o-uY_dAjZ37YHuRMEyzh8Tq-90JHQvicOqx",
  "d": "hR6HfxlTwcjMGST5wYnkGiJvuVnpUPbvXSGsvwjJhUM"
}
```


Another example of a different JWK for the BLS12381 curve where the public key is in the G2 subgroup.


```
{
  "kty": "EC",
  "crv": "BLS12381G2",
  "x": "Atx1GqJH4rXlpTk0wg9LA6SsHrWWdPPqL2BXLd7zzMpFLeLdr-QQMJ2NPebFkw-h
CyWIj8dwP9uvuu9c9WZrVWvQnY2n7xQHF-BM-Mx6747t_ZJCu809fskA3ca3TVr7",
  "y": "Bk0BZG3RijbTl9YqzuAZZHuxj4eNxKBF4TD_6KdxmCxgAri0Bx46xtcMqqKgqUmd
DRC65Jv08EkVBojJkraUVEkxVhixgYS5hdfRfYZWaisT4M_NYoOFZFP4_5Jg05_p",
  "d": "1jeo0uurZvaIC82YUMNLOHalfvhabbMHtLeVaI0tNhs"
}
```


A.2. BLS48581 Key Pairs

The following examples showcase JWKs for both the G1 and G2 subgroups of the BLS48581 curve. As before, note that the examples also include the corresponding private key, expressed through the inclusion of the “d” parameter.

An example JWK for the BLS48581 curve where the public key is in the G1 subgroup.

```
{
  "kty": "EC",
  "crv": "BLS48581G1",
  "x": "BZo5kuiunkAUaE9n-c8L12pjTfV35ZTzei0eYIzYEM05Y--PCABHPXt20ImhyL9K
sdrUqYxe5KrsbsahKYdN9dXa6a7fsFnWxw",
  "y": "EJfIRJ62OJ1vnLuwtziSgC4syIDVgiYoGxqLhdryqJEGepP7-4iePB5nrAthL6gl
MeKIeF9q7jsZfeM3g4CTlXMOH2yLCh1VyA",
  "d": "FbigQBwP9gNCFI_LFxt-c8ZpgY_1JjSOx-oUweZJgmGYZijWUsL6R0qQY1gwtrHT
LWEWNbq--FlOVKL_EBlbL9I"
}
```


Another example of a different JWK for the BLS48581 curve where the public key is in the G1 subgroup.


```
{
  "kty": "EC",
  "crv": "BLS48581G1",
  "x": "BjRT7VST4vMlTj6yMF73QlEg5XSHYQflAJMPf-4BhjO9qL8A6Rqo1OsdiGTrC3jY
S3mLOHp-zg-yDmK_7HD8RR4S9j2Tf84blA",
  "y": "BOS-o0BD7RI7t2w5q0ljpy9NRJ7h8vT-sjfj8HKpGXaVP17RFUswlc1dBSVPsiSZ
RU78ZinNO0kK57dJrDXeRUB7gSM6L6aZog",
  "d": "pAq4V50JFEVjNbx12WDpHCiolrB-wxQw6wOZh2l_5-p_TWfTui7LgcIBpZb17idK
gSh-XhGqhxEkXMUggGOQjJc"
}
```


An example JWK for the BLS48581 curve where the public key is in the G2 subgroup.

```
{
  "kty": "EC",
  "crv": "BLS48581G2",
  "x": "ANAdJhZscIOfuf06ScGr1EwKcy7IFnq4bKPRl_QpBhRtx7Hg4hvpCXXbt03L1UGv
oZbf-pxVfOyQMaA1qsGAHU0R6OYgUIpc-wE3KKZFLtzfS3vKPVLSLNTm7USw7audlChzhn8g
aG5aJc1J7j0SfN0pn5TPLVA6PE47cMhHWHEirUzpkFxLTKYNqNoQVOZxuqcJs6UAC9ZwJaIi
vfDvv4XJuS02y7irAjJxhXhWfF9TuTyp6aiyGU1mjiYAoJ6HSIaJ2TiR5UztoiMjuUuOqZG4
Rof5FuPGD665DvCmNurtsHM_KiT9gcJerJ_LbvJt-fqEIgEOnXCFlpcbxP0zoComUVEqzk-A
rZ-a58hUVV0J6-7Y1lXJYDaqQPOX_YEiLrtudwfuoPz0iWLezmcI3bPx6g71SOjSQ7SiHU_k
HG7IpWkg4uIq9zpQ_U66giDqmoglccwoMMyeG_LAd7zsuILtzOwPJOjJkC4U3HcAVZvSLQZz
9dk1tuXR8ZfGuX1YHeTO6Hx-SA9Lz0F9yKJMBCUgd9ltimLO5JkzV3jGgin3IIHjM-XqEVFr
tGCq0L775LRhmVg4CAb4bHaqvN2XW7mWordv9EvHq7NRwCVzMPFYWUd2-sXgqJ3AU0l5Bqpn
gjH3gxSnG7mNEnmctmjQSnSOYhBoWRzmoJ2FmtQEFxCVIZvL7ZCaqkD27ZjamowAKFzmdFWV
-wzHSs-br6ely00z402C7iX5c85zsI9NqxMwkDpprpx5oGjIFqiO8kkDyPdJSoLfzPA",
  "y": "DhTWwVEjNmqbRMtXexiuMVQEvL_ZqLk0NcjlzrlqO-k8uiRmKxiupQ8-Qm1tKYUJ
sJVdkLiyL14ptu0BbNoFIxUqLIP3PtauAgZjdSgUPOqDz7xvEaHGIhcEdivoKwokBpLQfO0x
CSoia3tBm37xFWTLYNmmQQR8AEpUPk4OP9IWn5XkJQGYUfraO2qwNUmDdJwIJb8pDZVp_A0x
YugO1CuKp-hlfNV6rdEYeGsYuMZelR9XlcNI9CdfsnQsfcoE5bypqeN5kJiCDNI0apdFQgxX
D5xipr-6OafMARtcJclLbOlqzYL4l0coAwVbBe1Yz54yPGu4ubBI5N4dZcZ43c46hMFh_hz3
qYkru5ClWjGtvRHUrBWNVTKoyyHAelBylnBckATeep2wHJmwE92fILQx-TQH3xYAwgx0o4ZC
4_2gZXr73zddtS7mxaxWm6Y6AbHAoIpUBrqcMd9QjZ4_lX6BR1P_TKL_HySHOd4RMM-3H1fw
e52V2E9Gi8tZJJzkLsWNT0F9MLYDULv1-4zRkPuKuqZGUfswU-cufNmx1U4TfrWpeqzwhQ8i
h74AH8Fygk7ZpPwLAqFr_FNPoXeoxlRP4426_8Rsw-9fMjlDW3qqdEMI1M25BEm9kglUW__r
n0OyFrCPfPDpUmlQxDmu50Uwi1m-8jnmGQxfDqzgrQqN79DUtD8C8m9y26zFttasdNMFEjE9
vlq6GVbpYEr3juZhvKBvLzJLGGRQrxxGDPDGA_itNRJnw_EtafcH4rkWDtWV4yb79Sw",
  "d": "x-6jzDQgIvWIEyd5PF6nq9DNTIFesIExG_jBMJd9HJMtQdfDooFlQvbY3Ts0rSb-
sPIIpLBx7bRCtwhkpioKmMM"
}
```


Another example of a different JWK for the BLS48581 curve where the public key is in the G2 subgroup.

```
{
  "kty": "EC",
  "crv": "BLS48581G2",
  "x": "BgaTERiH8qDLfouNR44GOkiE2EOCgCbLxWEI3ocyXPLxeEtCCVUtnj3sQv-I3nM3
V6IptFAoEJkLpCmMLBwyMTZ3B69p61yYBAU-fO2XyUiR0aEmWgqI-tesctbExIleiWWi221n
wzIVUKi47E6bkNnBjvynvHMaB4lsJ0llYlsuYO7QqKXY55xSatMbTkTFncEOeEjQbDjHu96O
DBD0F9r2-yahJ2PW5Jaztt9B0-UtHlTz0nje_ZaRTarna3-2p9ZrWM6DpXJQJg1dvefE1ngk
7wJK0Agl0XQ8B0kKd3kkomO1CygV7MKN_OyKOJB2k4Vouv4i5MCC6GzIjUnF8vkakzzW-Fja
hSgKl1_QsvBrVSNwrGxpamhjpNn1Jx_FLbH2FAlE3Qv2sCveeEEoDGZ5qk1FbGhQFSicUlLh
XymY1xBxMyqhoNPVy6_utYgeM9MPU9UtylGShAoIuE7qjzwH5OKY9rKj7z2z39gBdH12X6Mo
Qwnn1zKQyhYyfHSmQcLN9Kmpke-5AQsNw0Oo8R05HhjhdR2GIWPIRHqCXN_cu__qof7jdtUu
pCoNUms3YyGMNYXdDEZzQS_8Fex6zWrHLCsTXqBrlAtKUIrzA-zAS_Jj_iIEvZRQM6J949P5
iSEbSOtIalYzUuoOIjbF2s7bWpwNwgvKL1LbHT_ldARL9y0RxeK5BINrKCLA9aDDpK4rQX1B
_ZR4ni422eQgfbdT6MjZ_YooobKKQxYCXdcx-DQsjhVMIHcr2RG_1450wmybP9Ycwpc",
  "y": "DoHzwzZAL1ArvHD-z7Eey67D4IEjfVgdXgANRGmtQzPirXDhOmohjnvMJ9KisyWm
kJKuSp5B0wr-EO4AmmPualDZNutOC97NzAk2tJeVi5kNWPKp1RKxHIDhAqME-LUbVCTRFn23
rfO9QNDd0dPev35o6ee3FwGtJYlieEeYEym0wHM96FxwfjsPrxgZYYorCToGES5rzbr1zOh0
vmLVei-n-VWOnjymKh6CzjGLZm7q8exB8QZoG_JeugV7l0GifG4eeLfh4hDtYVNH7JCeJJEN
jfgDdp1Dy1fHDv7U9bX8gDEfRoTJS9FDU85a-tc3c5Oy472IzIq-Aml39YolBPISU1gNRO5R
PK4gMad184pxtrYXZaMWOow3I2aUSDZ0-IBH4QLP8MSJoVxZHo5fhkpkSlFT1C5FgNiNny_I
48EtANkHjH4S8zOxegLeTxK9doj2k6c2ptNAR7xDdm2mhfNhKIRgev3vhW70W54QpUpckS9i
znbOl6ofzs-CtSezA7yMhLh_Vb0bgz6Wz2viixI6jd9_yVkicPse-57Fi24Et0x3A1CnuWkw
Ez1TvXk-9QWFQWKhAsoIMCB0svCjgcnSKcaAeRFGvd0XKtBICmHhCK1CqvcAuYtsDELmhzsi
JVxOpmB5JdgDt2Ii6CaiAzxkP-I02O6UbdzGbZPN0gJfgIJRMuvJRZF-G9An1CsTMD6Y0Q4R
o3aWrSY3mpnKRZddVC2W4OKuhS7qrLR7REl-gJvSCzaqiuLQlvqOrP4i55n52tDVWqQ",
  "d": "TeLY_9dGUWdbaMjjgWA8-osKXvyfPz3gq4B9Drr-dV0ZgB3hhYBWlkklKOuO78t8
FUCypARd4bpHGKJmsPafn8A"
}
```


Appendix B. COSE_Key Examples

B.1. BLS12381 Key Pairs

The following examples showcase COSE_key examples for both the G1 and G2 subgroups of the BLS12381 curve. Note, the examples also include the corresponding private key, expressed through the inclusion of the “d” (-4) parameter.

An example COSE_Key for the BLS12381 curve where the public key is in the G1 subgroup expressed as an octet string.


```
a50101200d21583011de060462d56ac129e1e8cfcf8e02be595b4e575f2cb726d9070826
5b812faa7f490991ad9bc935add8689f96c7c22622583001b75802c01bdb4087ce5556e9
504ef62d7a05c18e99c62230b941121f437c0883bbfd59200775cdec128bd7fae75ee023
5820de773afecdfc1555656b06f098f14e8c1e139403f2fcad93c77f48ed79c49c37
```


Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 13,
  -2: h'11DE060462D56AC129E1E8CFCF8E02BE595B4E575F2CB726D90708265B812FAA
7F490991AD9BC935ADD8689F96C7C226',
  -3: h'01B75802C01BDB4087CE5556E9504EF62D7A05C18E99C62230B941121F437C08
83BBFD59200775CDEC128BD7FAE75EE0',
  -4: h'DE773AFECDFC1555656B06F098F14E8C1E139403F2FCAD93C77F48ED79C49C37
}
```

Another example of a different COSE_Key for the BLS12381 curve where the public key is in the G1 subgroup expressed as an octet string.

```
a50101200d215830114190131a73c5e6f099711ea9cdfd388dc9d4d7d408c5503ea73f2d
bfb874bbb4c42692addd2b0c131316d85de6bfb622583014da577e9e1afb937b09be76f2
9c1184b20d3a6c32ba18ca8cfcfc8dc6b180248d6426e369842c1a83a17ed46a58aa6023
582039d341ad10eef3d22b9e56391e5fb6096fb772a5b4470ec881052ec0b67c815e
```

Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 13,
  -2: h'114190131A73C5E6F099711EA9CDFD388DC9D4D7D408C5503EA73F2DBFB874BB
B4C42692ADDD2B0C131316D85DE6BFB6',
  -3: h'14DA577E9E1AFB937B09BE76F29C1184B20D3A6C32BA18CA8CFCFC8DC6B18024
8D6426E369842C1A83A17ED46A58AA60',
  -4: h'39D341AD10EEF3D22B9E56391E5FB6096FB772A5B4470EC881052EC0B67C815E
}
```

An example COSE_Key for the BLS12381 curve where the public key is in the G2 subgroup expressed as an octet string.

```
a50101200e215860019003f72fb13e7f03f922fe6b1843a8e7fcdaf47031c5d007a32af7
43779a14c4664c602825810fdc71d3e03510a423015a595ea2a0a900d5ede9fef8b19a0e
35d0e29843a0622a7cb13edc3a001bdb12e45b16b60274d28dfba48253b34d2122586014
75166c12064581d08975ee393472f329860fcec9a64b63dcf36af39e94466a77622ef08d
0ebb092b5f7c7327a2352f06abeff3e0d8959f1f00276a96b7f02082798d84097cae4711
9a14e450f7d93fb99fd597a10c0ff8c0563a25c2967455235820890ec57aacf4d641c4b6
19a78774f9b814a50f5858aafd56ec038739e96f834f
```

Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 14,
  -2: h'019003F72FB13E7F03F922FE6B1843A8E7FCDAF47031C5D007A32AF743779A14
C4664C602825810FDC71D3E03510A423015A595EA2A0A900D5EDE9FEF8B19A0E35D0E298
43A0622A7CB13EDC3A001BDB12E45B16B60274D28DFBA48253B34D21',
  -3: h'1475166C12064581D08975EE393472F329860FCEC9A64B63DCF36AF39E94466A
77622EF08D0EBB092B5F7C7327A2352F06ABEFF3E0D8959F1F00276A96B7F02082798D84
097CAE47119A14E450F7D93FB99FD597A10C0FF8C0563A25C2967455',
  -4: h'890EC57AACF4D641C4B619A78774F9B814A50F5858AAFD56EC038739E96F834F
}
```

Another example of a different COSE_Key for the BLS12381 curve where the public key is in the G2 subgroup expressed as an octet string.

```
a50101200e21586003b81526b001b41701632609ee1285cf09549e2228caa0775a052ae6
f1ae5737dcc66a8c0f0b65fac070d85b0217cc6c0ce5db1c27767ef73f2e8355b5f02dab
a2b810548fc8f0be26c329375b95b6b6d844ce981ced5934709e57aca986f92722586010
97125da5ebd6b31d875a3884c2197b1afcdecbbbbc26871e38880fe80eac09c6e754e865
a9f01b3ed511d86673a6d8109dc94d0840ff539fa2d175b2dea6bd3484d91a73424ad4c4
acc9cc748fb5280477a5c187dc6d749d0de00beee1a2062358202a9cff87262ce1b09303
2446ac6911c4b947305deea7631e23d1a27c46bd9f62
```

Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 14,
  -2: h'03B81526B001B41701632609EE1285CF09549E2228CAA0775A052AE6F1AE5737
DCC66A8C0F0B65FAC070D85B0217CC6C0CE5DB1C27767EF73F2E8355B5F02DABA2B81054
8FC8F0BE26C329375B95B6B6D844CE981CED5934709E57ACA986F927',
  -3: h'1097125DA5EBD6B31D875A3884C2197B1AFCDECBBBBC26871E38880FE80EAC09
C6E754E865A9F01B3ED511D86673A6D8109DC94D0840FF539FA2D175B2DEA6BD3484D91A
73424AD4C4ACC9CC748FB5280477A5C187DC6D749D0DE00BEEE1A206',
  -4: h'2A9CFF87262CE1B093032446AC6911C4B947305DEEA7631E23D1A27C46BD9F62
}
```

B.2. BLS48581 Key Pairs

The following examples showcase COSE_key examples for both the G1 and G2 subgroups of the BLS48581 curve. Note, the examples also include the corresponding private key, expressed through the inclusion of the “d” (-4) parameter.

An example COSE_Key for the BLS48581 curve where the public key is in the G1 subgroup expressed as an octet string.

```
a50101200f2158490522e96ca7ca18bf31598a15d39aa95c6fe56da85a7bc8e8108f193c
54ea68c84b973ed2f29725ed7a1413329699258050e2c69628d83d0cc4b83bb10fafae7f
a535ad21a1fef91eaf225849003b9940c85d62aba1e9955d6b1836d01bad300b886d0ae9
7df1305b0bfbca337fad9662581647ca6cf11b861e3e71642d5d82c254774fb67937a237
45c2d1f328898a53eac0cad87e2358416e9dcfdc9abd54a06233f8b0d49ef665362ebf45
39a8d83fe273b4c54ff36e8b600823e2695560e4615d9a866e929b918e8183fa89660c1f
e684e3bd671cf29ece
```

Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 15,
  -2: h'0522E96CA7CA18BF31598A15D39AA95C6FE56DA85A7BC8E8108F193C54EA68C8
4B973ED2F29725ED7A1413329699258050E2C69628D83D0CC4B83BB10FAFAE7FA535AD21
A1FEF91EAF',
  -3: h'003B9940C85D62ABA1E9955D6B1836D01BAD300B886D0AE97DF1305B0BFBCA33
7FAD9662581647CA6CF11B861E3E71642D5D82C254774FB67937A23745C2D1F328898A53
EAC0CAD87E',
  -4: h'6E9DCFDC9ABD54A06233F8B0D49EF665362EBF4539A8D83FE273B4C54FF36E8B
600823E2695560E4615D9A866E929B918E8183FA89660C1FE684E3BD671CF29ECE'
}
```

Another example of a different COSE_Key for the BLS48581 curve where the public key is in the G1 subgroup expressed as an octet string.

```
a50101200f215849063453ed5493e2f3254e3eb2305ef7425120e574876107e500930f7f
ee018633bda8bf00e91aa8d4eb1d8864eb0b78d84b798b387a7ece0fb20e62bfec70fc45
1e12f63d937fce1b9422584904e4bea34043ed123bb76c39ab4963a72f4d449ee1f2f4fe
b237e3f072a91976953f5ed1154b3095cd5d05254fb22499454efc6629cd3b490ae7b749
ac35de45407b81233a2fa699a2235841a40ab8579d0914456335bc75d960e91c28a896b0
7ec31430eb039987697fe7ea7f4d67d3ba2ecb81c201a596f5ee274a81287e5e11aa8711
245cc5208063908c97
```

Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 15,
  -2: h'063453ED5493E2F3254E3EB2305EF7425120E574876107E500930F7FEE018633
BDA8BF00E91AA8D4EB1D8864EB0B78D84B798B387A7ECE0FB20E62BFEC70FC451E12F63D
937FCE1B94',
  -3: h'04E4BEA34043ED123BB76C39AB4963A72F4D449EE1F2F4FEB237E3F072A91976
953F5ED1154B3095CD5D05254FB22499454EFC6629CD3B490AE7B749AC35DE45407B8123
3A2FA699A2',
  -4: h'A40AB8579D0914456335BC75D960E91C28A896B07EC31430EB039987697FE7EA
7F4D67D3BA2ECB81C201A596F5EE274A81287E5E11AA8711245CC5208063908C97'
}
```

An example COSE_Key for the BLS48581 curve where the public key is in the G2 subgroup expressed as an octet string.

```
a501012010215902480 0d01d26166c70839fb9fd3a49c1abd44c0a732ec8167ab86ca3d1
97f42906146dc7b1e0e21be90975dbb74dcbd541afa196dffa9c557cec9031a035aac180
1d4d11e8e620508a5cfb013728a6452edcdf4b7bca3d52d22cd4e6ed44b0edab9d942873
867f20686e5a25cd49ee3d127cdd299f94cf2d503a3c4e3b70c847587122ad4ce9905c4b
4ca60da8da1054e671baa709b3a5000bd67025a222bdf0efbf85c9b92d36cbb8ab023271
8578567c5f53b93ca9e9a8b2194d668e2600a09e87488689d93891e54ceda22323b94b8e
a991b84687f916e3c60faeb90ef0a636eaedb0733f2a24fd81c25eac9fcb6ef26df9fa84
22010e9d708596971bc4fd33a02a2651512ace4f80ad9f9ae7c854555d09ebeed8d655c9
6036aa40f397fd81222ebb6e7707eea0fcf48962dece6708ddb3f1ea0ef548e8d243b4a2
1d4fe41c6ec8a56920e2e22af73a50fd4eba8220ea9a882571cc2830cc9e1bf2c077bcec
b882edccec0f24e8c9902e14dc7700559bd22d0673f5d935b6e5d1f197c6b97d581de4ce
e87c7e480f4bcf417dc8a24c04252077d96d8a62cee499335778c68229f72081e333e5ea
11516bb460aad0befbe4b4619958380806f86c76aabcdd975bb996a2b76ff44bc7abb351
c0257330f158594776fac5e0a89dc053497906aa678231f78314a71bb98d12799cb668d0
4a748e621068591ce6a09d859ad404171095219bcbed909aaa40f6ed98da9a8c00285ce6
745595fb0cc74acf9bafa7a5cb4d33e34d82ee25f973ce73b08f4dab1330903a69ae9c79
a068c816a88ef24903c8f7494a82dfccf0225902480e14d6c15123366a9b44cb577b18ae
315404bcbfd9a8b93435c8e5ceb96a3be93cba24662b18aea50f3e426d6d298509b0955d
90b8b22f5e29b6ed016cda0523152a2c83f73ed6ae0206637528143cea83cfbc6f11a1c6
221704762be82b0a240692d07ced31092a226b7b419b7ef11564cb60d9a641047c004a54
3e4e0e3fd2169f95e425019851fada3b6ab0354983749c0825bf290d9569fc0d3162e80e
d42b8aa7e8657cd57aadd118786b18b8c65e951f5795c348f4275fb2742c7dca04e5bca9
a9e3799098820cd2346a9745420c570f9c62a6bfba39a7cc011b5c25c94b6ce96acd82f8
97472803055b05ed58cf9e323c6bb8b9b048e4de1d65c678ddce3a84c161fe1cf7a9892b
bb90a55a31adbd11d4ac158d5532a8cb21c07a507296705c9004de7a9db01c99b013dd9f
20b431f93407df1600c20c74a38642e3fda0657afbdf375db52ee6c5ac569ba63a01b1c0
a08a5406ba9c31df508d9e3f957e814753ff4ca2ff1f248739de1130cfb71f57f07b9d95
d84f468bcb59249ce42ec58d4f417d30b60350bbf5fb8cd190fb8abaa64651fb3053e72e
7cd9b1d54e137eb5a97aacf0850f2287be001fc172824ed9a4fc0b02a16bfc534fa177a8
c6544fe38dbaffc46cc3ef5f3239435b7aaa744308d4cdb90449bd9209545bffeb9f43b2
16b08f7cf0e9526950c439aee745308b59bef239e6190c5f0eace0ad0a8defd0d4b43f02
f26f72dbacc5b6d6ac74d30512313dbe5aba1956e9604af78ee661bca06f2f324b186450
af1c460cf0c603f8ad351267c3f12d69f707e2b9160ed595e326fbf52c235841c7eea3cc
342022f5881327793c5ea7abd0cd4c815eb081311bf8c130977d1c932d41d7c3a2816542
f6d8dd3b34ad26feb0f208a4b071edb442b70864a62a0a98c3
```

Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 16,
  -2: h'00D01D26166C70839FB9FD3A49C1ABD44C0A732EC8167AB86CA3D197F4290614
6DC7B1E0E21BE90975DBB74DCBD541AFA196DFFA9C557CEC9031A035AAC1801D4D11E8E6
20508A5CFB013728A6452EDCDF4B7BCA3D52D22CD4E6ED44B0EDAB9D942873867F20686E
5A25CD49EE3D127CDD299F94CF2D503A3C4E3B70C847587122AD4CE9905C4B4CA60DA8DA
1054E671BAA709B3A5000BD67025A222BDF0EFBF85C9B92D36CBB8AB0232718578567C5F
53B93CA9E9A8B2194D668E2600A09E87488689D93891E54CEDA22323B94B8EA991B84687
F916E3C60FAEB90EF0A636EAEDB0733F2A24FD81C25EAC9FCB6EF26DF9FA8422010E9D70
8596971BC4FD33A02A2651512ACE4F80AD9F9AE7C854555D09EBEED8D655C96036AA40F3
97FD81222EBB6E7707EEA0FCF48962DECE6708DDB3F1EA0EF548E8D243B4A21D4FE41C6E
C8A56920E2E22AF73A50FD4EBA8220EA9A882571CC2830CC9E1BF2C077BCECB882EDCCEC
0F24E8C9902E14DC7700559BD22D0673F5D935B6E5D1F197C6B97D581DE4CEE87C7E480F
4BCF417DC8A24C04252077D96D8A62CEE499335778C68229F72081E333E5EA11516BB460
AAD0BEFBE4B4619958380806F86C76AABCDD975BB996A2B76FF44BC7ABB351C0257330F1
58594776FAC5E0A89DC053497906AA678231F78314A71BB98D12799CB668D04A748E6210
68591CE6A09D859AD404171095219BCBED909AAA40F6ED98DA9A8C00285CE6745595FB0C
C74ACF9BAFA7A5CB4D33E34D82EE25F973CE73B08F4DAB1330903A69AE9C79A068C816A8
8EF24903C8F7494A82DFCCF0',
  -3: h'0E14D6C15123366A9B44CB577B18AE315404BCBFD9A8B93435C8E5CEB96A3BE9
3CBA24662B18AEA50F3E426D6D298509B0955D90B8B22F5E29B6ED016CDA0523152A2C83
F73ED6AE0206637528143CEA83CFBC6F11A1C6221704762BE82B0A240692D07CED31092A
226B7B419B7EF11564CB60D9A641047C004A543E4E0E3FD2169F95E425019851FADA3B6A
B0354983749C0825BF290D9569FC0D3162E80ED42B8AA7E8657CD57AADD118786B18B8C6
5E951F5795C348F4275FB2742C7DCA04E5BCA9A9E3799098820CD2346A9745420C570F9C
62A6BFBA39A7CC011B5C25C94B6CE96ACD82F897472803055B05ED58CF9E323C6BB8B9B0
48E4DE1D65C678DDCE3A84C161FE1CF7A9892BBB90A55A31ADBD11D4AC158D5532A8CB21
C07A507296705C9004DE7A9DB01C99B013DD9F20B431F93407DF1600C20C74A38642E3FD
A0657AFBDF375DB52EE6C5AC569BA63A01B1C0A08A5406BA9C31DF508D9E3F957E814753
FF4CA2FF1F248739DE1130CFB71F57F07B9D95D84F468BCB59249CE42EC58D4F417D30B6
0350BBF5FB8CD190FB8ABAA64651FB3053E72E7CD9B1D54E137EB5A97AACF0850F2287BE
001FC172824ED9A4FC0B02A16BFC534FA177A8C6544FE38DBAFFC46CC3EF5F3239435B7A
AA744308D4CDB90449BD9209545BFFEB9F43B216B08F7CF0E9526950C439AEE745308B59
BEF239E6190C5F0EACE0AD0A8DEFD0D4B43F02F26F72DBACC5B6D6AC74D30512313DBE5A
BA1956E9604AF78EE661BCA06F2F324B186450AF1C460CF0C603F8AD351267C3F12D69F7
07E2B9160ED595E326FBF52C',
  -4: h'C7EEA3CC342022F5881327793C5EA7ABD0CD4C815EB081311BF8C130977D1C93
2D41D7C3A2816542F6D8DD3B34AD26FEB0F208A4B071EDB442B70864A62A0A98C3'
}
```

Another example of a different COSE_Key for the BLS48581 curve where the public key is in the G2 subgroup expressed as an octet string.

a501012010215902480606931118 87f2a0cb7e8b8d478e063a4884d843828026cbc56108
de87325cf2f1784b4209552d9e3dec42ff88de733757a229b4502810990ba4298c2c1c32
31367707af69eb5c9804053e7ced97c94891d1a1265a0a88fad7ac72d6c4c4895e8965a2
db6d67c3321550a8b8ec4e9b90d9c18efca7bc731a07896c274965625b2e60eed0a8a5d8
e79c526ad31b4e44c59dc10e7848d06c38c7bbde8e0c10f417daf6fb26a12763d6e496b3
b6df41d3e52d1e54f3d278defd96914daae76b7fb6a7d66b58ce83a57250260d5dbde7c4
d67824ef024ad00825d1743c07490a777924a263b50b2815ecc28dfcec8a389076938568
bafe22e4c082e86cc88d49c5f2f91a933cd6f858da85280a975fd0b2f06b552370ac6c69
6a6863a4d9f5271fc52db1f6140944dd0bf6b02bde7841280c6679aa4d456c685015289c
5252e15f2998d71071332aa1a0d3d5cbafeeb5881e33d30f53d52dca5192840a08b84eea
8f3c07e4e298f6b2a3ef3db3dfd801747d765fa3284309e7d73290ca16327c74a641c2cd
f4a9a991efb9010b0dc343a8f11d391e18e1751d862163c8447a825cdfdcbbffeaa1fee3
76d52ea42a0d526b3763218c3585dd0c4673412ffc15ec7acd6ac72c2b135ea06b940b4a
508af303ecc04bf263fe2204bd945033a27de3d3f989211b48eb486a563352ea0e2236c5
dacedb5a9c0dc20bca2f52db1d3fe574044bf72d11c5e2b904836b2822c0f5a0c3a4ae2b
417d41fd94789e2e36d9e4207db753e8c8d9fd8a28a1b28a4316025dd731f8342c8e154c
20772bd911bfd78e74c26c9b3fd61cc297225902480e81f3c336402f502bbc70fecfb11e
cbaec3e081237d581d5e000d4469ad4333e2ad70e13a6a218e7bcc27d2a2b325a69092ae
4a9e41d30afe10ee009a63ee6a50d936eb4e0bdecdcc0936b497958b990d58f2a9d512b1
1c80e102a304f8b51b5424d1167db7adf3bd40d0ddd1d3debf7e68e9e7b71701ad258962
7847981329b4c0733de85c707e3b0faf1819618a2b093a06112e6bcdbaf5cce874be62d5
7a2fa7f9558e9e3ca62a1e82ce318b666eeaf1ec41f106681bf25eba057b9741a27c6e1e
78b7e1e210ed615347ec909e24910d8df803769d43cb57c70efed4f5b5fc80311f4684c9
4bd14353ce5afad7377393b2e3bd88cc8abe026977f58a2504f21253580d44ee513cae20
31a775f38a71b6b61765a3163a8c37236694483674f88047e102cff0c489a15c591e8e5f
864a644a5153d42e4580d88d9f2fc8e3c12d00d9078c7e12f333b17a02de4f12bd7688f6
93a736a6d34047bc43766da685f3612884607afdef856ef45b9e10a54a5c912f62ce76ce
97aa1fcecf82b527b303bc8c84b87f55bd1b833e96cf6be28b123a8ddf7fc9592270fb1e
fb9ec58b6e04b74c770350a7b96930133d53bd793ef505854162a102ca08302074b2f0a3
81c9d229c680791146bddd172ad0480a61e108ad42aaf700b98b6c0c42e6873b22255c4e
a6607925d803b76222e826a2033c643fe234d8ee946ddcc66d93cdd2025f80825132ebc9
45917e1bd027d42b13303e98d10e11a37696ad26379a99ca45975d542d96e0e2ae852eea
acb47b44497e809bd20b36aa8ae2d096fa8eacfe22e799f9dad0d55aa42358414de2d8ff
d74651675b68c8e381603cfa8b0a5efc9f3f3de0ab807d0ebafe755d19801de185805696
492528eb8eefcb7c1540b2a4045de1ba4718a266b0f69f9fc0

Below is the above CBOR rendered in diagnostic view.

```
{
  1: 1,
  -1: 16,
  -2: h'060693111887F2A0CB7E8B8D478E063A4884D843828026CBC56108DE87325CF2
F1784B4209552D9E3DEC42FF88DE733757A229B4502810990BA4298C2C1C3231367707AF
69EB5C9804053E7CED97C94891D1A1265A0A88FAD7AC72D6C4C4895E8965A2DB6D67C332
1550A8B8EC4E9B90D9C18EFCA7BC731A07896C274965625B2E60EED0A8A5D8E79C526AD3
1B4E44C59DC10E7848D06C38C7BBDE8E0C10F417DAF6FB26A12763D6E496B3B6DF41D3E5
2D1E54F3D278DEFD96914DAAE76B7FB6A7D66B58CE83A57250260D5DBDE7C4D67824EF02
4AD00825D1743C07490A777924A263B50B2815ECC28DFCEC8A389076938568BAFE22E4C0
82E86CC88D49C5F2F91A933CD6F858DA85280A975FD0B2F06B552370AC6C696A6863A4D9
F5271FC52DB1F6140944DD0BF6B02BDE7841280C6679AA4D456C685015289C5252E15F29
98D71071332AA1A0D3D5CBAFEEB5881E33D30F53D52DCA5192840A08B84EEA8F3C07E4E2
98F6B2A3EF3DB3DFD801747D765FA3284309E7D73290CA16327C74A641C2CDF4A9A991EF
B9010B0DC343A8F11D391E18E1751D862163C8447A825CDFDCBBFFEAA1FEE376D52EA42A
0D526B3763218C3585DD0C4673412FFC15EC7ACD6AC72C2B135EA06B940B4A508AF303EC
C04BF263FE2204BD945033A27DE3D3F989211B48EB486A563352EA0E2236C5DACEDB5A9C
0DC20BCA2F52DB1D3FE574044BF72D11C5E2B904836B2822C0F5A0C3A4AE2B417D41FD94
789E2E36D9E4207DB753E8C8D9FD8A28A1B28A4316025DD731F8342C8E154C20772BD911
BFD78E74C26C9B3FD61CC297',
  -3: h'0E81F3C336402F502BBC70FECFB11ECBAEC3E081237D581D5E000D4469AD4333
E2AD70E13A6A218E7BCC27D2A2B325A69092AE4A9E41D30AFE10EE009A63EE6A50D936EB
4E0BDECDCC0936B497958B990D58F2A9D512B11C80E102A304F8B51B5424D1167DB7ADF3
BD40D0DDD1D3DEBF7E68E9E7B71701AD2589627847981329B4C0733DE85C707E3B0FAF18
19618A2B093A06112E6BCDBAF5CCE874BE62D57A2FA7F9558E9E3CA62A1E82CE318B666E
EAF1EC41F106681BF25EBA057B9741A27C6E1E78B7E1E210ED615347EC909E24910D8DF8
03769D43CB57C70EFED4F5B5FC80311F4684C94BD14353CE5AFAD7377393B2E3BD88CC8A
BE026977F58A2504F21253580D44EE513CAE2031A775F38A71B6B61765A3163A8C372366
94483674F88047E102CFF0C489A15C591E8E5F864A644A5153D42E4580D88D9F2FC8E3C1
2D00D9078C7E12F333B17A02DE4F12BD7688F693A736A6D34047BC43766DA685F3612884
607AFDEF856EF45B9E10A54A5C912F62CE76CE97AA1FCECF82B527B303BC8C84B87F55BD
1B833E96CF6BE28B123A8DDF7FC9592270FB1EFB9EC58B6E04B74C770350A7B96930133D
53BD793EF505854162A102CA08302074B2F0A381C9D229C680791146BDDD172AD0480A61
E108AD42AAF700B98B6C0C42E6873B22255C4EA6607925D803B76222E826A2033C643FE2
34D8EE946DDCC66D93CDD2025F80825132EBC945917E1BD027D42B13303E98D10E11A376
96AD26379A99CA45975D542D96E0E2AE852EEAACB47B44497E809BD20B36AA8AE2D096FA
8EACFE22E799F9DAD0D55AA4',
  -4: h'4DE2D8FFD74651675B68C8E381603CFA8B0A5EFC9F3F3DE0AB807D0EBAFE755D
19801DE185805696492528EB8EEFCB7C1540B2A4045DE1BA4718A266B0F69F9FC0'
}
```

Appendix C. Acknowledgments

The authors would like to acknowledge the work of Kyle Den Hartog, which was used as the foundation for this draft. We would also like to thank David Waite for his contributions to the specification.

Appendix D. Document History

-05

*Replaced instances of "Bls" with "BLS" since B., L., and S. are people's initials, just like "RSA" is three people's initials.

-04

*Changed the key type from OKP to EC/EC2 since these keys use "x" and "y" values.

-03

*Updated references.

-02

*Update COSE_Key and JWK examples.

-01

*Added JWK examples.

-00

*Created draft-ietf-cose-bls-key-representations-00 from draft-looker-cose-bls-key-representations-00 following working group adoption.

Authors' Addresses

Tobias Looker
Mattr

Email: tobias.looker@mattr.global

Michael B. Jones
Self-Issued Consulting

Email: michael_b_jones@hotmail.com
URI: https://self-issued.info/