



Red Hat Enterprise Linux Release 9.2 Manual Pages on 'jose-jwk-gen.1' command

\$ man jose-jwk-gen.1

JOSE-JWK-GEN(1) JOSE-JWK-GEN(1)

NAME

jose-jwk-gen - Creates a random JWK for each input JWK template

SYNOPSIS

jose jwk gen -i JWK [-o JWK]

OVERVIEW

The jose jwk gen command generates a key from one or more JWK(Set) templates. If a single template is given as input, a single JWK will be output. However, if multiple templates are given as input, a single JWKSet will be output containing all the keys.

The best way to generate a key is to specify the algorithm it will be used with in the "alg" property of the JWK template. This method should be preferred since, when generating from an algorithm, an appropriate "key_ops" parameter will be emitted automatically. Further, having a JWK with the algorithm already specified will assist algorithm inference when encrypting or signing.

Alternatively, you can generate a key by specifying its key type ("kty") JWK property, along with the required type-specific generation parameter. See the examples below for how to do this for each key type.

If the type-specific generation parameter is non-standard (for example: "bytes" and "bits"), it will be removed excluded from the output.

OPTIONS

? -i JSON, --input=JSON : Parse JWK(Set) template from JSON

- ? -i FILE, --input=FILE : Read JWK(Set) template from FILE
- ? -i -, --input=- : Read JWK(Set) template from standard input
- ? -o FILE, --output=FILE : Write JWK(Set) to FILE
- ? -o -, --output=- : Write JWK(Set) to standard input
- ? -s, --set : Always output a JWKSet

EXAMPLES

Generate three keys, each targeting a different algorithm:

```
$ jose jwk gen -i '{"alg":"HS256"}' -o oct.jwk
```

```
$ jose jwk gen -i '{"alg":"RS256"}' -o rsa.jwk
```

```
$ jose jwk gen -i '{"alg":"ES256"}' -o ec.jwk
```

Generate three keys using key parameters rather than algorithms:

```
$ jose jwk gen -i '{"kty":"oct","bytes":32}' -o oct.jwk
```

```
$ jose jwk gen -i '{"kty":"RSA","bits":4096}' -o rsa.jwk
```

```
$ jose jwk gen -i '{"kty":"EC","crv":"P-256"}' -o ec.jwk
```

Create multiple keys at once using a JWKSet template:

```
$ jose jwk gen \
-i '{"keys":[{"alg":"HS256"}, {"alg":"ES256"}]}' \
-o keys.jwkset
```

Create multiple keys at once using multiple JWK templates:

```
$ jose jwk gen \
-i '{"alg":"HS256"}' \
-i '{"alg":"ES256"}' \
-o keys.jwkset
```

AUTHOR

Nathaniel McCallum <npmccallum@redhat.com>

SEE ALSO

jose-alg(1), jose-jwe-dec(1), jose-jwe-enc(1), jose-jwk-exc(1),
jose-jwk-pub(1), jose-jwk-thp(1), jose-jwk-use(1), jose-jws-sig(1),
jose-jws-ver(1),

08/09/2021

JOSE-JWK-GEN(1)