Rocky Enterprise Linux 9.2 Manual Pages on command 'jose-jwk-exc.1'

$ man jose-jwk-exc.1

JOSE-JWK-EXC(1) JOSE-JWK-EXC(1)

NAME

jose-jwk-exc - Performs a key exchange using the two input keys

SYNOPSIS

jose jwk exc [-i JWK] -l JWK -r JWK [-o JWK]

OVERVIEW

The jose jwk exc command performs a key exchange using the two input keys and provides the result of the exchange as output. The user can specify a JWK template as input and the specified properties will appear in the output JWK unmodified.

A key exchange requires two keys:

1. The local key, which usually contains private key material.
2. The remote key, which usually contains public key material.

The algorithm for the exchange is inferred from the inputs.

The ECDH algorithm performs a standard elliptic curve multiplication such that the public value of \p rem is multiplied by the private value of \p.

The ECMR algorithm has three modes of operation. Where the local key

has a private key (the "d" property), it performs exactly like ECDH. If the local key does not have a private key and the remote key does have a private key, elliptic curve addition is performed on the two values. Otherwise, if neither the local key nor the remote key have a private key, the remote key is subtracted from the local key using elliptic curve subtraction. When using ECMR, be sure to validate the content of your inputs to avoid triggering the incorrect operation!

OPTIONS

- -i JSON, --input=JSON : Parse JWK template from JSON
- -i FILE, --input=FILE : Read JWK template from FILE
- -i -, --input=- : Read JWK template from standard input
- -o FILE, --output=FILE : Write JWK(Set) to FILE
- -o -, --output=- : Write JWK(Set) to standard input
- -l FILE, --local=FILE : Read local JWK from FILE
- -l -, --local=- : Read local JWK from standard input
- -r FILE, --remote=FILE : Read remote JWK from FILE
- -r -, --remote=- : Read remote JWK from standard input

EXAMPLES

Perform a key exchange:

```
$ jose jwk gen -i '{"alg":"ECDH"}' -o local.jwk
$ jose jwk gen -i '{"alg":"ECDH"}' | jose jwk pub -i- -o remote.jwk
$ jose jwk exc -l local.jwk -r remote.jwk -o exchanged.jwk
```

AUTHOR

Nathaniel McCallum <npmccallum@redhat.com>

SEE ALSO

jose-alg(1), jose-jwk-exc(1), jose-jwk-gen(1), jose-jwk-pub(1)