Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'jose-jwe-dec.1' command

$ man jose-jwe-dec.1

JOSE-JWE-DEC(1) JOSE-JWE-DEC(1)

NAME

jose-jwe-dec - Decrypts a JWE using the supplied JWKs

SYNOPSIS

jose jwe dec -i JWE [-I CT] -k JWK [-p] [-O PT]

OVERVIEW

The jose jwe dec command decrypts a JWE using one or more JWK (-k) or password (-p). Decryption succeeds if any key is able to perform decryption.

If the JWE is a detached JWE, meaning that the ciphertext is stored in binary form external to the JWE itself, the ciphertext can be loaded using the -I parameter.

Please note that, when specifying the -O option to output the plaintext, plaintext output begins before ciphertext validation. Therefore, you must check the return value of the command before using the data.

OPTIONS

- -i JSON, --input=JSON : Parse JWE from JSON
- -i FILE, --input=FILE : Read JWE from FILE
- -i -, --input=- : Read JWE from standard input
- -I FILE, --detached=FILE : Read decoded ciphertext from FILE
- -I -, --detached=- : Read decoded ciphertext from standard input
- -p, --password : Prompt for a decryption password, if necessary

? -k FILE, --key=FILE : Read JWK(Set) from FILE

? -k -, --key=- : Read JWK(Set) from standard input

? -O JSON, --detach=JSON : Parse JWE from JSON

? -O FILE, --detach=FILE : Read JWE from FILE

? -O -, --detach=- : Read JWE from standard input

EXAMPLES

Decrypt a JWE with a JWK:

```
$ jose jwe dec -i msg.jwe -k rsa.key -O msg.txt
```

Decrypt a JWE with a password:

```
$ jose jwe dec -i msg.jwe -p -O msg.txt
Please enter decryption password:
```

Decrypt a JWE with either of two JWKs:

```
$ jose jwe dec -i msg.jwe -k ec.jwk -k rsa.jwk -O msg.txt
```

AUTHOR

Nathaniel McCallum <npmccallum@redhat.com>

SEE ALSO

jose-jwe-enc(1), jose-jwe-fmt(1)