



Red Hat Enterprise Linux Release 9.2 Manual Pages on 'jose-jws-ver.1' command

\$ man jose-jws-ver.1

JOSE-JWS-VER(1) JOSE-JWS-VER(1)

NAME

jose-jws-ver - Verifies a JWS using the supplied JWKs

SYNOPSIS

jose jws ver -i JWS [-I PAY] -k JWK [-a] [-O PAY]

OVERVIEW

The jose jws ver command verifies a signature over a payload using one or more JWKs. When specifying more than one JWK (-k), the program will succeed when any of the provided JWKs successfully verify a signature.

Alternatively, if the -a option is given, the program will succeed only when all JWKs successfully verify a signature.

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

Please note that, when specifying the -O option to output the payload, the payload is output whether or not the signature validates.

Therefore, you must check the return value of the command before trusting the data.

OPTIONS

- ? -i JSON, --input=JSON : Parse JWS from JSON
- ? -i FILE, --input=FILE : Read JWS from FILE
- ? -i -, --input=- : Read JWS from standard input
- ? -I FILE, --detached=FILE : Read decoded payload from FILE

- ? -l -, --detached=- : Read decoded payload from standard input
- ? -k FILE, --key=FILE : Read JWK(Set) from FILE
- ? -k -, --key=- : Read JWK(Set) from standard input
- ? -O FILE, --detach=FILE : Decode payload to FILE
- ? -O -, --detach=- : Decode payload to standard output
- ? -a, --all : Ensure the JWS validates with all keys

EXAMPLES

Verify a regular JWS and output the payload:

```
$ jose jws ver -i msg.jws -k key.jwk -O msg.txt
```

Verify a detached JWS without outputting the payload:

```
$ jose jws ver -i msg.jws -l msg.txt -k key.jwk
```

Ensure that a JWS is signed with all specified keys:

```
$ jose jws ver -i msg.jws -k ec.jwk -k rsa.jwk -a
```

AUTHOR

Nathaniel McCallum <npmccallum@redhat.com>

SEE ALSO

jose-jws-fmt(1), jose-jws-sig(1)

08/09/2021

JOSE-JWS-VER(1)