



Rocky Enterprise Linux 9.2 Manual Pages on command 'sshpk-verify.1'

C:~>man sshpk-verify.1

SSHPK-VERIFY() SSHPK-VERIFY()

NAME

sshpk-verify - verify a signature on data using an SSH key

SYNOPSIS

sshpk-verify -i KEYPATH -s SIGNATURE [OPTION...]

DESCRIPTION

Takes in arbitrary bytes and a Base64-encoded signature, and verifies that the signature was produced by the private half of the given SSH public key.

EXAMPLES

```
$ printf 'foo' | sshpk-verify -i ~/.ssh/id_ecdsa -s MEUCIQCYp...
```

OK

```
$ printf 'foo' | sshpk-verify -i ~/.ssh/id_ecdsa -s GARBAGE...
```

NOT OK

EXIT STATUS

0

Signature validates and matches the key.

1

Signature is parseable and the correct length but does not match the key or otherwise is invalid.

2

The signature or key could not be parsed.

3

Invalid commandline options were supplied.

OPTIONS

`-v, --verbose`

Print extra information about the key and signature to stderr when verifying.

`-i KEY, --identity=KEY`

Select the key to be used for verification. KEY must be a relative or absolute filesystem path to the key file. Any format supported by the sshpk library is supported, including OpenSSH formats and standard PEM PKCS.

`-s BASE64, --signature=BASE64`

Supplies the base64-encoded signature to be verified.

`-f PATH, --file=PATH`

Input file to verify instead of stdin.

`-H HASH, --hash=HASH`

Set the hash algorithm to be used for signing. This should be one of sha1, sha256 or sha512. Some key types may place restrictions on which hash algorithms may be used (e.g. ED25519 keys can only use SHA-512).

`-t FORMAT, --format=FORMAT`

Choose the signature format to use, from asn1, ssh or raw (only for ED25519 signatures). The asn1 format is the default, as it is the format used with TLS and typically the standard in most non-SSH libraries (e.g. OpenSSL). The ssh format is used in the SSH protocol and by the ssh-agent.

SEE ALSO

`sshpk-sign(1)`

BUGS

Report bugs at Github <https://github.com/arekinath/node-sshpk/issues>

January 2020

SSHPK-VERIFY()