NAME

sshpk−sign − sign data using an SSH key

SYNOPSYS

sshpk−sign −i KEYPATH [OPTION...]

DESCRIPTION

Takes in arbitrary bytes, and signs them using an SSH private key. The key can be of any type or format supported by the **sshpk** library, including the standard OpenSSH formats, as well as PEM PKCS#1 and PKCS#8.

The signature is printed out in Base64 encoding, unless the **−−binary** or **−b** option is given.

EXAMPLES

Signing with default settings:

```
$ printf ’foo’ | sshpk−sign −i ˜/.ssh/id_ecdsa
MEUCIAMdLS/vXrrtWFepwe...
```

Signing in SSH (RFC 4253) format (rather than the default ASN.1):

```
$ printf ’foo’ | sshpk−sign −i ˜/.ssh/id_ecdsa −t ssh
AAAAFGVjZHNhLXNoYTIt...
```

Saving the binary signature to a file:

```
$ printf ’foo’ | sshpk−sign −i ˜/.ssh/id_ecdsa \
                      −o signature.bin −b
$ cat signature.bin | base64
MEUCIAMdLS/vXrrtWFepwe...
```

OPTIONS

−v, −−verbose
Print extra information about the key and signature to stderr when signing.

−b, −−binary
Don’t base64−encode the signature before outputting it.

−i KEY, −−identity=KEY
Select the key to be used for signing. **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.

−f PATH, −−file=PATH
Input file to sign instead of stdin.

−o PATH, −−out=PATH
Output file to save signature in instead of stdout.

−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−verify(1)

BUGS

Report bugs at Github *https://github.com/arekinath/node−sshpk/issues*