NAME

openpgp2ssh — translate OpenPGP keys to SSH keys

SYNOPSIS

openpgp2ssh < mykey.gpg

gpg --export $KEYID | **openpgp2ssh $KEYID**

gpg --export $KEYID | **openpgp2pem $KEYID**

gpg --export $KEYID | **openpgp2spki $KEYID**

gpg --export-secret-key $KEYID | **openpgp2ssh $KEYID**

DESCRIPTION

openpgp2ssh takes an OpenPGP-formatted primary key and associated subkeys on standard input, and spits out the requested equivalent SSH-style (or PEM-encoded) key on standard output.

If the data on standard input contains no subkeys, you can invoke **openpgp2ssh** without arguments. If the data on standard input contains multiple keys (e.g. a primary key and associated subkeys), you must specify a specific OpenPGP key identifier as the first argument to indicate which key to export. The key ID is normally the 40 hex digit OpenPGP fingerprint of the key or subkey desired, but **openpgp2ssh** will accept as few as the last 8 digits of the fingerprint as a key ID.

If the input contains an OpenPGP RSA public key, it will be converted to the OpenSSH-style single-line keystring, prefixed with the key type ('ssh-rsa'). This format is suitable (with minor alterations) for insertion into known_hosts files and authorized_keys files. If invoked as 'openpgp2pem', a PEM-encoded public key will be emitted instead.

If invoked as 'openpgp2spki', a PEM-encoded subjectPublicKeyInfo (as defined in the X.509 standard) will be emitted instead.

If the input contains an OpenPGP RSA secret key, it will be converted to the equivalent PEM-encoded private key.

openpgp2ssh is part of the monkeysphere(7) framework for providing a PKI for SSH.

CAVEATS

The keys produced by this process are stripped of all identifying information, including certifications, self-signatures, etc. This is intentional, since ssh attaches no inherent significance to these features.

openpgp2ssh will produce output for any requested RSA key. This means, among other things, that it will happily export revoked keys, unverifiable keys, expired keys, etc. Make sure you do your own key validation before using this tool!

EXAMPLES

gpg --export-secret-key $KEYID | **openpgp2ssh $KEYID** | **ssh-add -c /dev/stdin**

This pushes the secret key into the active ssh-agent(1). Tools such as ssh(1) which know how to talk to the ssh-agent(1) can now rely on the key.

AUTHOR

openpgp2ssh and this man page were written by Daniel Kahn Gillmor <dkg@fifthhorseman.net>.

BUGS

openpgp2ssh only works with RSA keys. DSA keys are the only other key type available in both OpenPGP and SSH, but they are currently unsupported by this utility.

openpgp2ssh only accepts raw OpenPGP packets on standard input. It does not accept ASCII-armored input. **openpgp2ssh** Currently only exports into formats used by the OpenSSH. It should support other key output formats, such as those used by `lsh`(1) and `putty`(1).

Secret key output is currently not passphrase-protected.

openpgp2ssh currently cannot handle passphrase-protected secret keys on input.

SEE ALSO

`pem2openpgp`(1), `monkeysphere`(1), `monkeysphere`(7), `ssh`(1), `monkeysphere-authentication`(8), `monkeysphere-host`(8)