

Re: [NMLUG] Signing a document with my SSH key, not a PGP key?

Re: [NMLUG] Signing a document with my SSH key, not a PGP key?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2006-12/msg01790.html>

- *From:* "Wesley J. Landaker" <wjl@xxxxxxxxxxxxxx>
 - *Date:* Fri, 29 Dec 2006 08:40:14 -0700
-

On Friday 29 December 2006 07:46, Kelly Jones wrote:

I want to sign a document with `~/.ssh/id_dsa` so that people who have my public SSH key (`~/.ssh/id_dsa.pub`) can confirm that it's from me. I don't want to encrypt the document, just sign it.

How can I do this? Is it a good idea? Does `ssh-keysign` (which is disabled by default) play into it?

I know how to sign things using a PGP key, but was wondering if an SSH key would work as well?

Which you can make a signature with pretty much any public key, signing things with an SSH key is a very ODD thing to do and doesn't have any support infrastructure.

If you really want to do it, see <http://search.cpan.org/~dbrobins/Net-SSH-Perl/lib/Net/SSH/Perl/Key/Dsa.pm> which basically just lets you wrap an SSH DSA key and sign with it. It won't make pretty cleartext signatures or whatnot.

If you instead really want to have a unified SSH/OpenPGP infrastructure, you could use <http://www.red-bean.com/~nemo/openssh-gpg/> which lets you login SSH with OpenPGP keys instead of standard SSH keys.

Or, just use the OpenPGP infrastructure for what it's meant for (encrypting, signing, web-of-trust), and use SSH keys for what they are meant for (point-to-point network authentication) and if you want to correlate them, you can sign your SSH key with your OpenPGP key.

—
Wesley J. Landaker <wjl@xxxxxxxxxxxxxx> <<xmpp:wjl@xxxxxxxxxxxxxx>>
OpenPGP FP: 4135 2A3B 4726 ACC5 9094 0097 F0A9 8A4C 4CD6 E3D2

Attachment: [pgph57AivsoKn.pgp](#)
Description: PGP signature

Re: [NMLUG] Signing a document with my SSH key, not a PGP key?