

Re: About PGP Signing a File.

Source: <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2007-02/msg01038.html>

- *From:* Tony Arnold <tony.arnold@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 13 Feb 2007 08:00:25 +0000
-

John L Fjellstad wrote:

Tony Arnold <tony.arnold@xxxxxxxxxxxxxxxxxxxx> writes:

It therefore becomes a question of degrees of trust. A document that has been signed with a key that has also been signed by a number of people increases that degree of trust, but as you say does not guarantee authorship. A signature based on a key that has not been signed by anybody is much less trustworthy.

I don't see how the number of people signing a key makes it more trustworthy unless you know at least one of the person who signed (and then you only actually need that one person's signing). A bad guy could just generate a bunch of new keys to sign the one key you are looking at.

Indeed that is true. In fact a really bad guy could generate a whole load of fake keys and use them to sign his own, which is why I said it wasn't guaranteed.

But on probability grounds a key signed by multiple people is likely to be more trustworthy than a totally unsigned key.

And if it's signed by someone you know or someone you can trust, then even better.

Phil Zimmerman, who invented PGP, used to sign keys at conventions etc or wherever he was appearing and I think you had to produce your passport before he would sign it. So, a key signed by Phil is likely to be reasonably trustworthy!

Regards,
Tony.

—

Re: About PGP Signing a File.

Tony Arnold, IT Security Coordinator, University of Manchester,
IT Services Division, Kilburn Building, Oxford Road, Manchester M13 9PL.
T: +44 (0)161 275 6093, F: +44 (0)870 136 1004, M: +44 (0)773 330 0039
E: tony.arnold@xxxxxxxxxxxxxxxxx, H: <http://www.man.ac.uk/Tony.Arnold>

—
ubuntu-users mailing list
ubuntu-users@xxxxxxxxxxxxxxxxx
Modify settings or unsubscribe at: <https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>