Key Signing Policy

Tuesday 3 March 2009 21:26

After a couple of key signing parties it looks like a have some kind of key signing policy:

1. Prior to a KSP I send my primary key ID 0x942CFFC4 to the organizers. This key is available on the keyservers, so that's all that's needed.
2. At the KSP I expect the organizers to provide a hardcopy of the list of fingerprints of the participants of the KSP. I don't have a printer, so I don't bother with hardcopies myself.
3. At the KSP I check the fingerprint listed as mine on the hardcopy provided to me against my fingerprint on my trusted GPG slip.
4. KSP style checking of the other fingerprints, checking them of on the hardcopy.
5. KSP style checking of IDs, checking them of on the hardcopy.
6. After the KSP keys with checked fingerprint and ID are fed to caff on the system that stores my primary key.
7. After the KSP the successfully checked keys are imported into my keyring, preferably from a keyring send by the organizers.

If every participant of the KSP does this everybody ends up with a bunch of encrypted keys containing signed keys in several mailboxes. The point of caff is that I don't really care what happens with the keys I've signed and sent. They could just be imported in a keyring so it enables trusted communication between me and that participant, or imported and released to a keyserver. That's up to the key signing policy of the participant to decide.

What I do is pipe every attachment through `gpg2 --import`, then do `gpg2 --send-key 942CFFC4`. If we then do a `gpg2 --refresh-keys` the signatures on our own key are synced, and the imported keys from the other members are updated, maybe including my sig. If my sig shows up through this route everything went ok and we can optionally add trust to that key to expand our web of trust.

by Roland van Ipenburg http://www.xs4all.nl/~ipenburg/blog/posts/dull/2009/03/03/key–signing–policy/