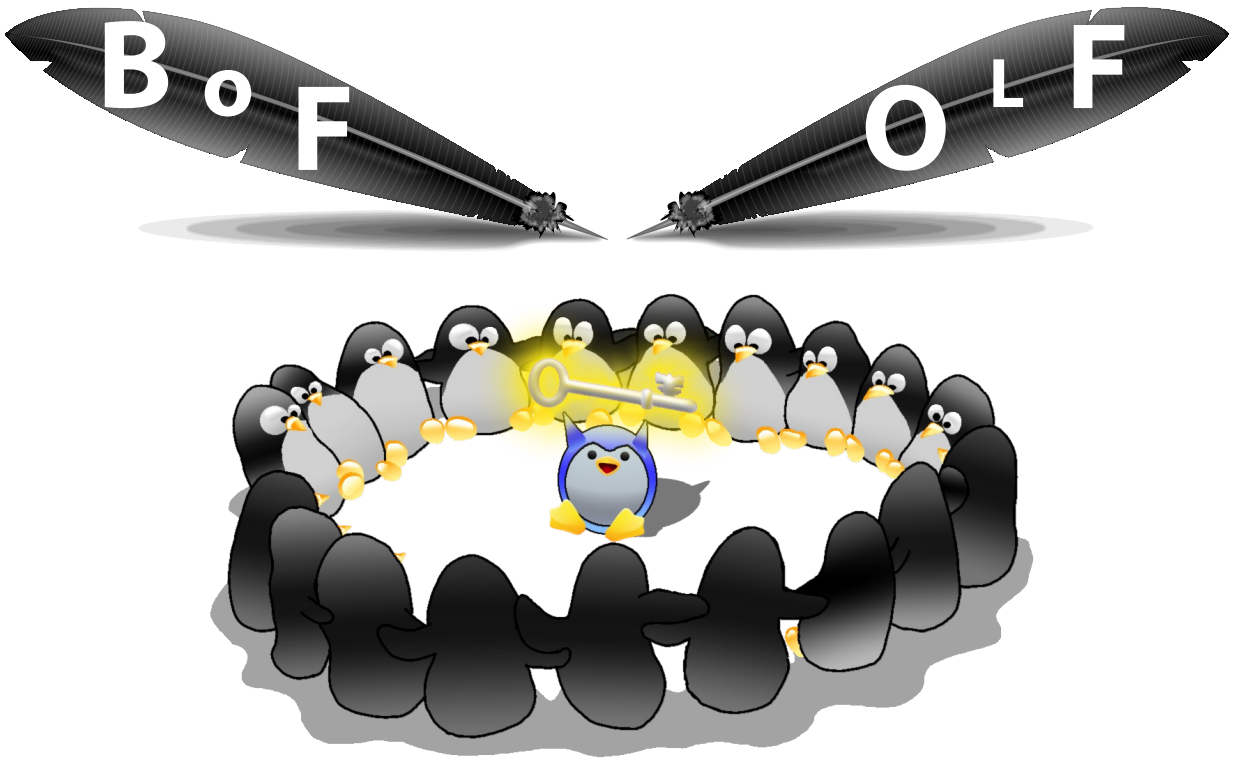

GPG/PGP Keysigning Party Instructions

6:00 PM Friday, October 24th

D242-243

OH/LinuxFest

Your Personal Web of Trust

If you are attending the OLF 2014 Key Signing, please send your public key (in "ascii armor" format) to rmt@casita.net prior to the meeting.

The GPG/PGP Keysigning Party for OLF 2014 is currently scheduled for 6PM Friday, October 24th, in D242-243.

Here's a quick rundown of how it works …

Before the Meeting

- install GnuPG (or other PGP workalike software)
- generate a key pair, if you have not already
- extract your public key and send it to the meeting organizer(s)
- extract your "fingerprint" and print a copy

During the Meeting

- bring your fingerprint
- bring additional paper and a pen or pencil
- bring a government issued photo ID
- read fingerprints (orally)
- check photo IDs (visually)

You do not need to bring a laptop or tablet or other device.
Computers are not needed during the meeting. It's all about face-to-face.

After the Meeting

- import the bundle of public keys (collected by the organizer)
- sign each participant's public key
- send each participant's signed key back to them
  -or-
- upload signed keys to a reputable public key server

"Can I just show up?" Yes, and please do. But the other participants will have to transcribe your fingerprint at the meeting, which will take more time.

Details follow, starting with easy steps for beginners.

Beginners

Install GnuPG. As root, issue one of the following commands ...

```
# for SUSE and OpenSUSE
zypper install gnupg

# for RedHat, Fedora, CentOS, Azure Duck
yum install gnupg

# for Debian or Ubuntu
apt-get install gnupg
```

Generate a key pair. As yourself, issue the command (and all others) ...

```
gpg --key-gen
```

When prompted, select RSA at 4096 bits.
Leave the "comment" blank, but enter your name and email address.
You can have multiple email addresses on your key. Your key will be referenced either by the key ID (a hexadecimal string) or by your email address.

NOTE: *remember your passphrase but do not share it with anyone*
NOTE: *protect your secret key (private key) and do not share it or upload it*

Extract your public key so that others can sign it.

```
gpg --armor --export you@yourdomain.tld > pubkeyfile.asc
```

Then send pubkeyfile.asc to the organizer(s).

Extract your key fingerprint.

```
gpg --fingerprint you@yourdomain.tld > fingerprint.txt
```

Then print fingerprint.txt and bring it with you to the meeting.

Tips

Key versus Key Pair

PGP/GPG keys are asymmetric. There is always a matched public key and private key, so what you have is a key *pair*. What gets signed by others in a key signing event is your public key. For that and other reasons, the terms "key" and "key pair" are often used interchangeably. When someone else uses your key, they're actually using your public key, for which there is one and only one private/secret counterpart.

Revocation Certificate

It is recommended that you create a revocation certificate. That way, if your private key or the passphrase is lost, you can revoke the public key. Otherwise, people might encrypt files or email with your public key that could never be decrypted.

Expiration Date

It's usually helpful to set an expiration date on your key. That way, if your the private key or the passphrase is lost, the public half will eventually become unusable and there will not be an ineffective public key in the grand web of trust. An expiration date is like an automatic revocation certificate. Expiration dates can be changed.

Multiple Keys

You can bring multiple keys to the meeting to be signed. (There are many reasons to have extra keys.) It means more fingerprints to read and more keys to sign, but the burden of additional keys weighs more on you more than on the group. If you bring two keys, we all have one additional key to sign, but you will have to double your signing of everyone else's key. The point is: don't feel guilty if you choose to do multiples.

Re-using your EMail Address

You can use a given email address on more than one PGP key, but selecting a particular key gets more difficult. This is not a problem if you get comfortable with using key IDs (the hexadecimal identifier).

Subkeys for Added Security

There is an excellent write-up on how to use subkeys at …

http://www.connexer.com/articles/openpgp-subkeys

Alternatives to Key Signing Party

A key signing party not the only way to share keys - consider "opportunistic signing" (easier than a key party). Be prepared to show your photo ID and share your fingerprint. Opportunistic key signing can be accomplished using something like a business card with your PGP fingerprint. When you learn that a friend or colleague also has a GPG/PGP key pair, then simply hand them your card and show them your DL or other legal identification. After face-to-face meeting you can exchange public keys electronically and sign with assurance (reviewing the physical media you swapped in person).

Using a Key Server

Most users of PGP upload their public key to one of the public key servers. The key servers communicate with each other, automatically synchronizing uploaded public keys. The best access is at http://hkps.pool.sks-keyservers.net/ which is the web interface. There is also a --keyserver flag on the 'gpg' command to.

Keybase.io

An exciting new service for publishing keys is Keybase.io. At first, it looks like a social networking site, but it's not for socializing. Keybase.io allows you to "prove" your key ownership by signing content on other sites. This is a form of statistical assurance: When you see several proofs of someone's key ownership you may choose to consider it valid.

Key Signing Follow-Through

After the meeting, be sure and perform the electronic signing you committed to. The organizer will prod participants to follow through with signing. It is discourteous to drop the ball and not finish the task.

Signing someone's key means you have viewed their government ID and checked their key fingerprint. It does not mean you vouch for their character or have any opinion about their personal integrity or trustworthiness or competence.

Sign all addresses on each participant's key.

The organizer(s) will …

- bring printed copy of all fingerprints available at press time
- send collected public keys to the group
- send one or more shell scripts to make key signing easier