KeySigning

All About Keys and Key Signing

Links

- The Apache reference on PGP key signing parties that take place at ApacheCon http://wiki.apache.org/apachecon/PgpKeySigning
- It points to this, which provides a really good overview, including how to create a key http://www.cryptnet.net/fdp/crypto/gpg-party.html
- Page under development on signing Apache releases http://wiki.apache.org/incubator/SigningReleases
- GnuPG, the GNU Privacy Guard page
 - http://gnupg.org
- The GNU Privacy Handbook, a forty-one page pdf document about GnuPG http://gnupg.org/gph/en/manual.pdf
- Everything you really need to know about keys, key signing, and signing releases at Apache KeysAtApache

How to Sign

Thanks to Jean Anderson for this description of the signing process:

The ApacheCon key signing only verifies the fingerprint and id of the person – everybody gets a hardcopy printout with name, email, and fingerprint. Incidentally, the "key id" is the last 8 digits of the fingerprint.

The electronic signing occurs later. Here are the steps somebody might use to sign my key.

- Import Jean's public key from pgp.mit.edu:
 - gpg --keyserver pgp.mit.edu --recv-keys 9958C626
- Verify the fingerprint does it exactly match the hardcopy from the ApacheCon key signing? gpg --fingerprint jta@apache.org
- 3. Sign Jean's key:
 - gpg --sign-key 9958C626
- 4. Upload the signed key:

gpg send-keys --keyserver pgp.mit.edu 9958C626

Another "style" is to not upload the signed key, but to export it and email it to the signee to upload (KEYID below is the id of the signer):

```
gpg --armor --export jta.apache.org > 9958C626_signed_by_KEYID
```

There's also a gpg-sign-keys.sh script available from dragon roe (https://dragon.roe.ch/bitsnpieces/scripts/gpg/gpg-sign-keys.sh-1.30), but it's best to understand what needs to be done before using somebody else's black box.