UCTrust PGP Key Signing Parties

UCTrust PGP Key Signing Parties

The UCTrust participants rely on PGP cryptographic signatures to verify the authenticity of electronic mail communications and federation metadata that are critical to the operation of UCTrust. In order to create the web of trust needed for this verification, key signing "parties" are conducted during UCTrust meetings. This document describes this key signing process.

1. Prior to the meeting, people who are not yet part of the web of trust should install PGP software, generate a public / private key pair, and upload the public key to one of the global PGP key servers, such as subkeys.pgp.net.
2. Everyone should bring a government-issued photo ID, such as a driver's license, as well as cards or slips of paper showing their public key ID and cryptographic fingerprint to the meeting. For example:

```
pub   1024D/6849ABF9 2007-07-25 [expires: 2012-07-23]
  Key fingerprint = 8B62 E459 6C53 3771 5C71  718F AD49 8EBB 6849 ABF9
uid                  David Walker <David.Walker@ucop.edu>
sub   4096g/51C3D427 2007-07-25 [expires: 2012-07-23]
```

1. During the key signing party itself, new members to the web of trust will go to all other meeting attendees, show them their photo ID and give them one of the slips of paper with the public key and fingerprint.
2. After the key signing party, everyone should retrieve the new members' public keys, sign them, and upload them back to one of the global PGP key servers.

For more information, see see Steve Lau's message, PGP Key Signing Party at UCITPS.