Key-Signing Party – Linuxwochen Wien 2014
Zimmermann-Sassaman Protocol

Stefan Huber

May 8, 2014
Checking fingerprints: the SHA256 checksum

6D18 F035 F611 BB5F CAC8 3217 5F3D D134
D2B4 BAC0 B154 52A9 76B8 06BD D99E 3D6F

- We know that we have the same file printed.
- Everyone testifies that his fingerprints on the list are OK!
Checking proof of identity
At home

- Import all keys to your local keyring.
- For each *checked* key on the list:
  - Compare the fingerprint of your copy with the fingerprint on the list.
  - Sign the key.
  - Mail the signed key to the owner.

Advanced hints:
- Install the package `signing-party`, which includes `caff`.
- `caff` automates fetching-signing-mailing keys.

*Signing someone else's key is an endorsement that you have first-hand evidence of the keyholder's identity. If you sign it when you don't really mean it, the Web of Trust can no longer be trusted.*

— [https://www.debian.org/events/keysigning](https://www.debian.org/events/keysigning)
Conventional key-signing

Person A:
- Gives person B a hardcopy of his fingerprint.
- Shows B a proof of identity.

Person B:
- Typically, puts a hand-written signature on each hardcopy.
- At home:
  - Fetch, verify, sign, and mail back the key.
  - See https://wiki.debian.org/Keysigning for the appropriate gpg commands.