Let's use Ed25519 with GnuPG 2.1 and Gnuik Token!

Niibe Yutaka
One of New Features in GnuPG 2.1

- ECC: Elliptic Curve Cryptography
  - New algorithm for public key crypto
- Benefit
  - Smaller key size for equivalent strength
- NOTE: It's not Post-quantum crypto
  - It can be broken by Shor's algorithm
ECC supported by GnuPG 2.1

- "Classic" ECC
  - Defined by some standard organizations
- "Modern" ECC
  - [https://safecurves.cr.yp.to/](https://safecurves.cr.yp.to/)
"Classic" ECC in GnuPG 2.1

- NIST Curves
  - P-256, P-384, P-521
- Brainpool
  - P-256, P-384, P-512
- secp256k1
  - Satoshi's Choice
- Feature
  - Too difficult to implement correctly
- Backdoor? Who knows?
"Modern" ECC in GnuPG 2.1

- GnuPG 2.1 supports:
  - Ed25519 for digital signature
  - X25519 for encryption/decryption
Let's start using Ed25519!

- ksp-dc17.txt: 4 / 142
- We know migration will take time
- When should we... ?
- Why not try something GNU today?
Need some reason?

- Gnuk supports Ed25519/X25519
  - It's faster than RSA
    - 0.1 sec for signature
    - 0.2 sec for decryption
  - Much safer against SCA
- OpenSSH supports Ed25519 auth
Gnuk BoF

- Gnuk is the USB security token implementation
- 10AM on Friday at Woody
Issues

• Not yet standardized
  • draft-ietf-openpgp-rfc4880bis-02
• SKS 1.1.6 supports Ed25519/X25519 keys
  • subset.pool.sks-keyservers.net
• Other keyservers don't support ECC keys yet
• wotsap does not yet support ECC keys
• alioth doesn't allow Ed25519 keys for SSH
HOWTO

- preparation
- key generation
- addkey
HOWTO: preparation

$ mkdir tmp/new-gpg-ecc
$ export GNUPGHOME=tmp/new-gpg-ecc
$ chmod og-rx $GNUPGHOME
$ gpg --version
HOWTO: key generation

```
$ gpg --expert --full-gen-key
```

Select '9' for "ECC and ECC".
Select '1' for 'Curve25519' to use Ed25519/X25519.
$ gpg --expert --edit-key chuji

[...

gpg> addkey

Select '11' for adding "Authentication" subkey for SSH. Toggle capability to "Authenticate" only: a->s->q

Select '1' for 'Curve25519' to use Ed25519/X25519. Type 'save' to save new subkey.
HOWTO: send-keys

Don't forget to add

```
--keyserver subset.pool.sks-keyservers.net
```
Questions?
Q1:
A1:
Questions?

Q1: Can I ask putting my Ed25519/X25519 key to debian-keyring?

A1: