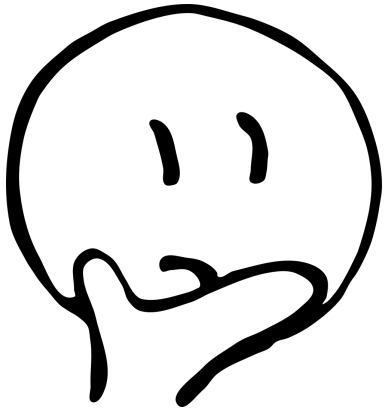
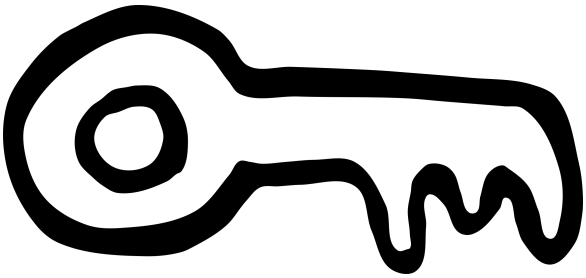
PGP Key Signing Party

Emil Miler, Pavel Dostál

Ilustrace: Terezka Tichá



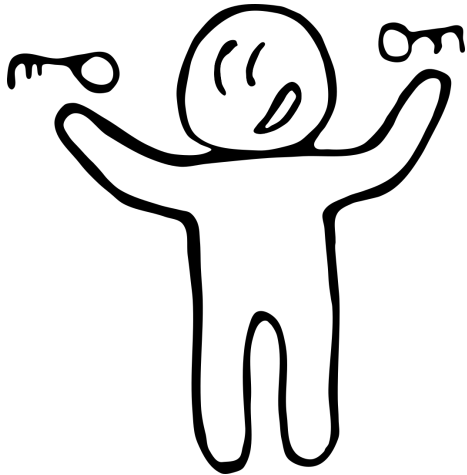


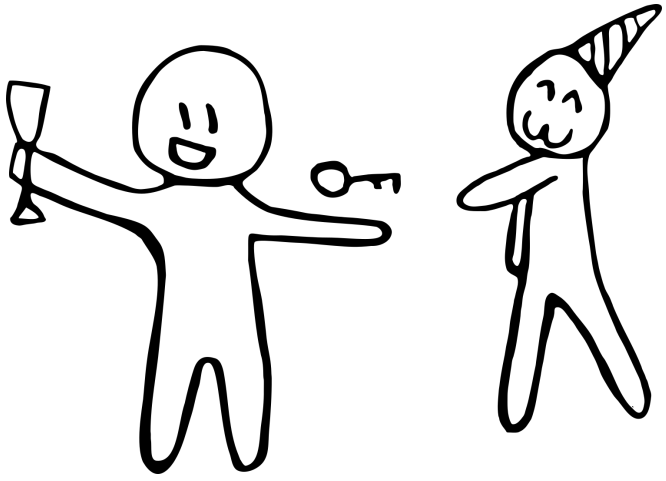
```
gpg --full-gen-key
```

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

RSA
4096 bit

Expirace, Jméno, Email, Komentář

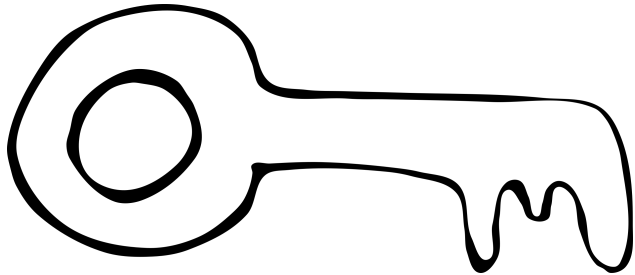


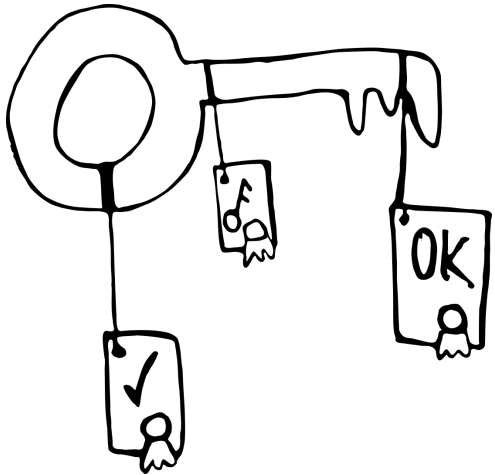


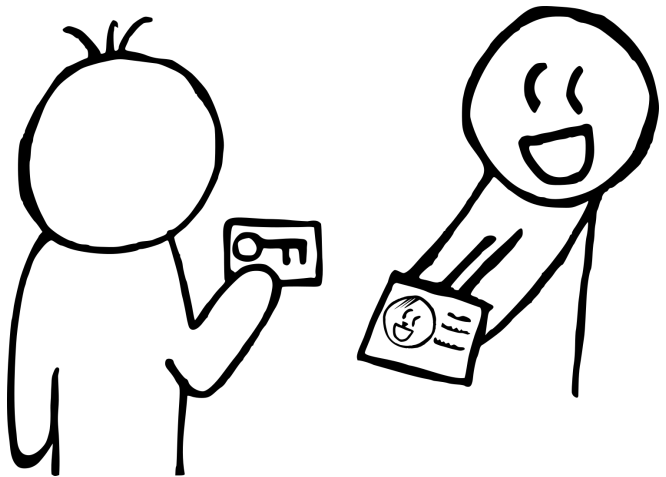
```
$ gpg -k

pub    rsa4096 2016-09-15 [SC] [expires:  2019-10-05]
       52C29D89915D03EC3F55F03523BB315BAB68B241
uid         [ultimate] Emil Miler <emil.miler@pedf.cuni.cz>
uid         [ultimate] Emil Miler <em@cocaine.ninja>
uid         [ultimate] Emil Miler <miler@gjk.cz>
sub    rsa4096 2016-09-15 [E] [expires:  2019-10-05]
```

```
gpg --edit-key 0xAB68B241

adduid
```

```
gpg --send-keys 0xAB68B241
```




OK

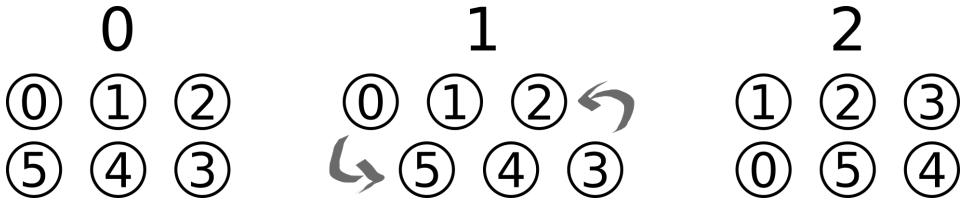


```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```


```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```

```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```

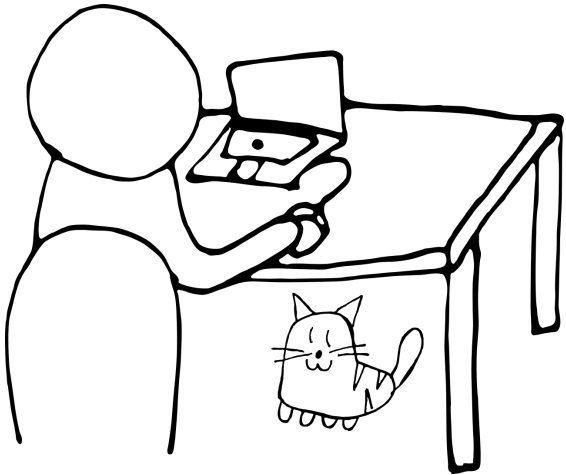
```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```


0
⓪ ① ②
⑤ ④ ③
1
⓪ ① ②
⑤ ④ ③
2
① ② ③
⓪ ⑤ ④

Během párty zkontrolovat:

- průkaz identity s fotografií
- adresy a otisk

```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```



- Stáhnout klíč z keyserveru
  - `gpg --keyserver pool.sks-keyservers.net --recv-keys <keyid>`
- Zkontrolovat otisk podle papírku
  - `gpg --fingerprint <keyid>`
- Podepsat správné identity
  - `gpg --sign-key --ask-cert-level <keyid>`
- Odeslat klíč majiteli
  - `gpg -a --export <keyid> | gpg -ear <keyid> > <keyfile>.asc`

linuxdays.cz/2018/key-signing-party