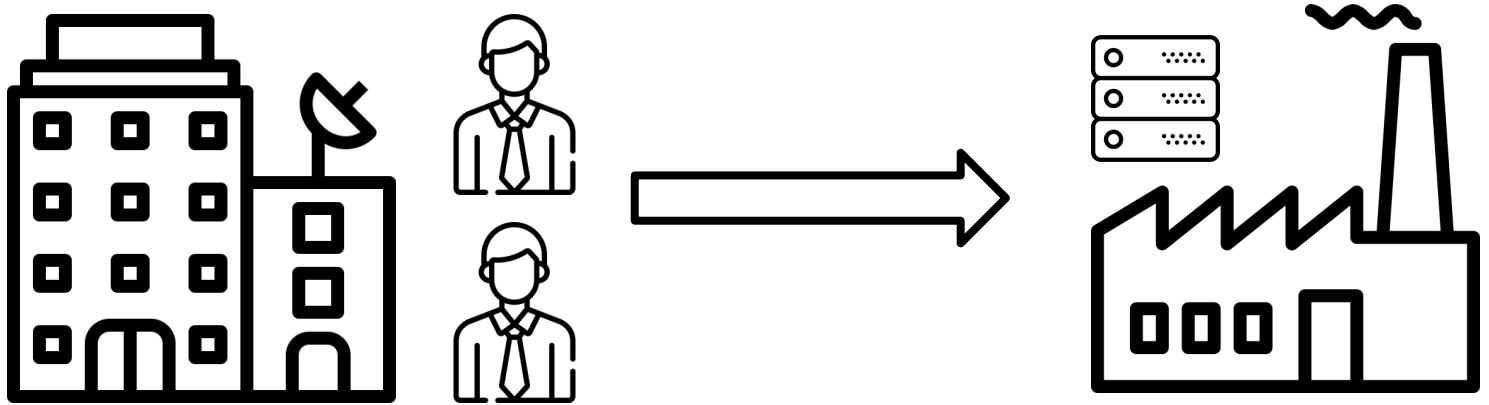
SSH Login With Signed Keys

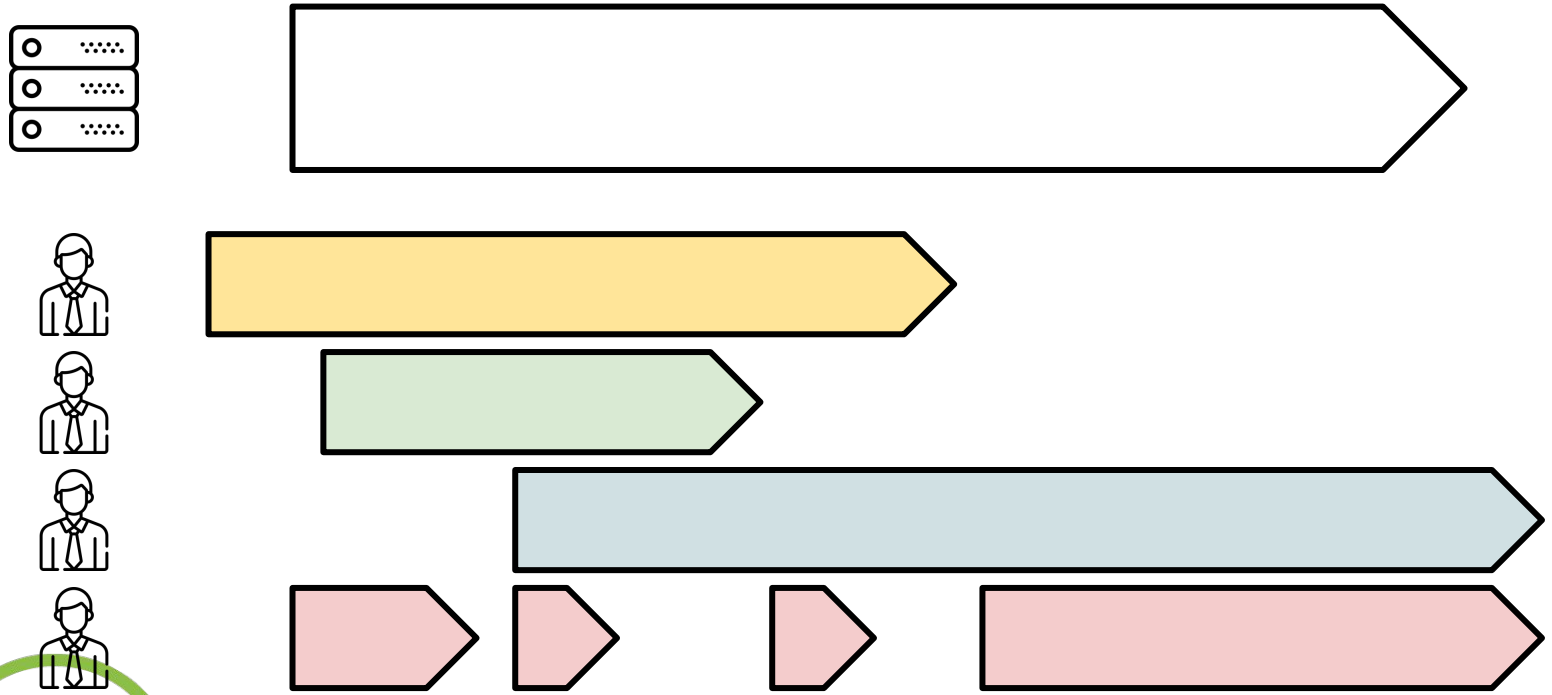
Jiří Kraml
LinuxDays 2019, Prague

No login, no service

- Usually no remote access



Lifecycle mismatch

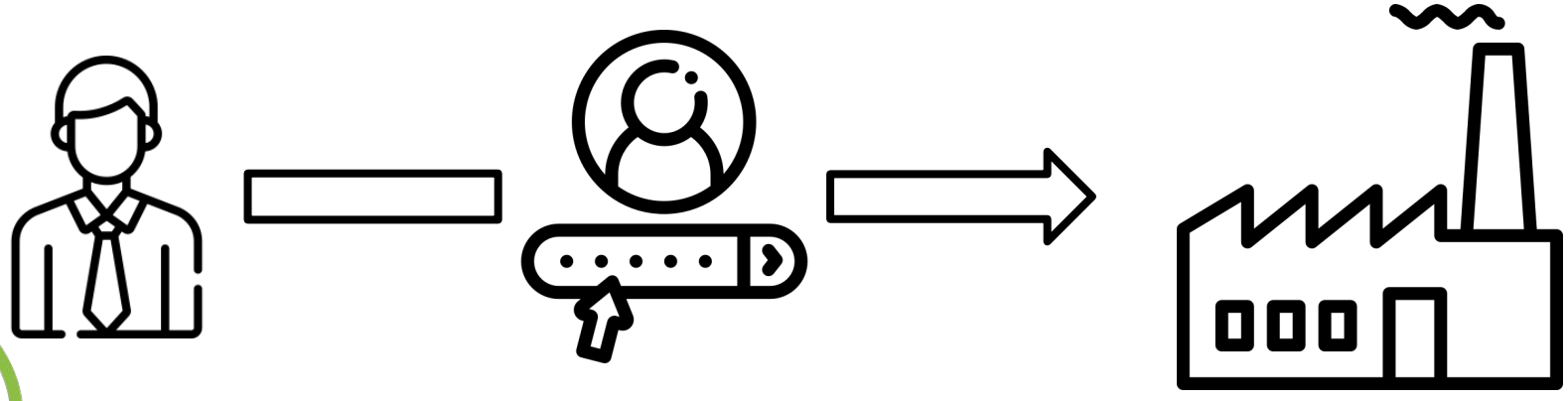


How can we log in?

- Password
- Key files
- Key files + certificate
- PAM

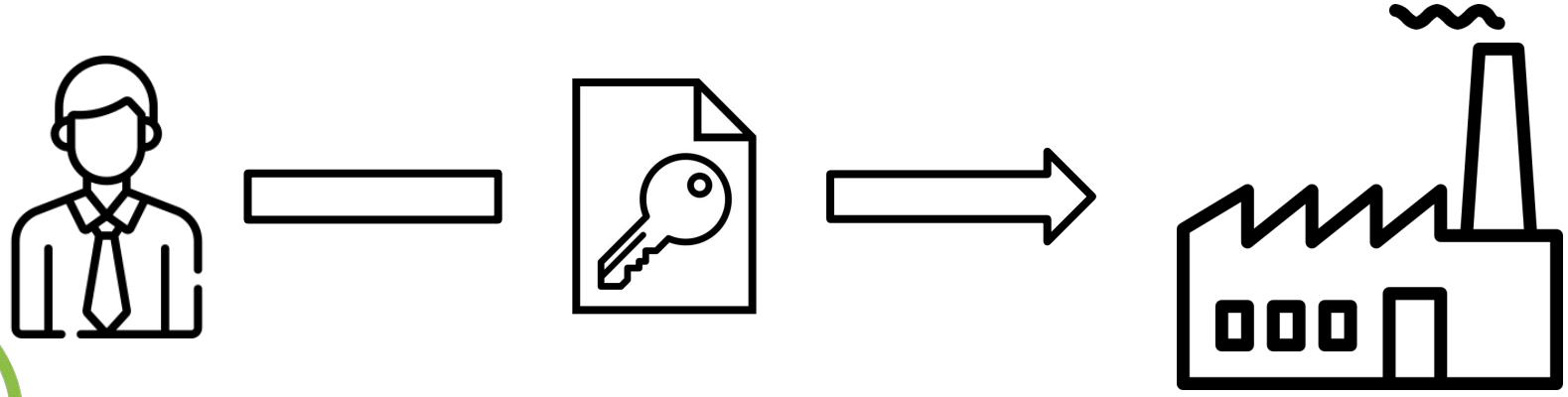
Password

- Usually only one account
  - Only one password, need to share it
  - Changes impact all users



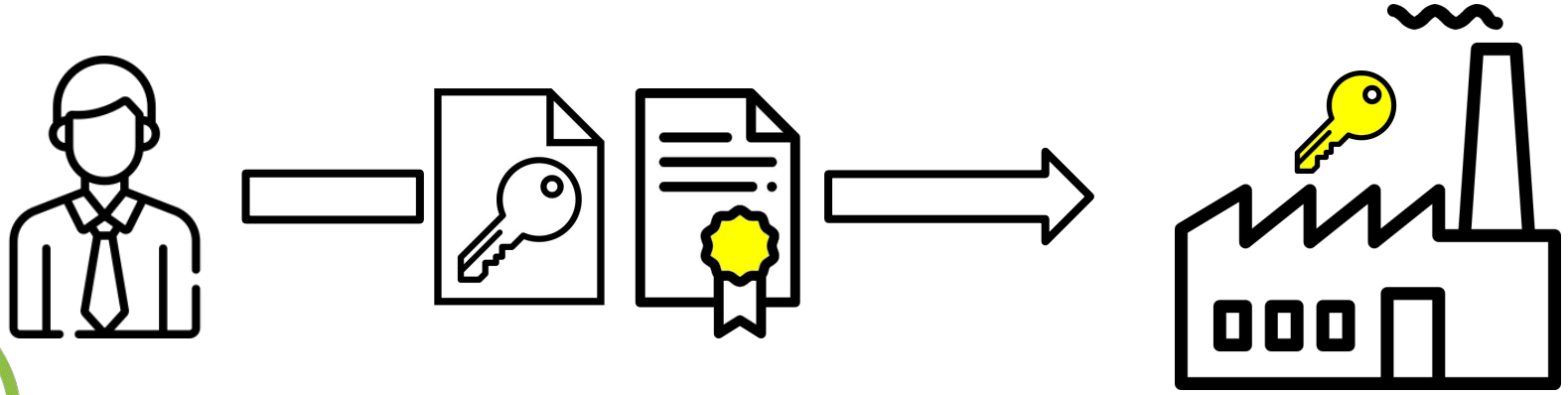
SSH keys

- Multiple keys per account possible
- Public key must be known on target host (`authorized_keys`)
- Keys are valid forever



Signed SSH keys

- The usual key pair, plus a certificate
  - “Signature Public Key” instead of `authorized_keys` file
- Arbitrary validity of certificate
- System clock accuracy is a security concern now
- OpenSSH Feature



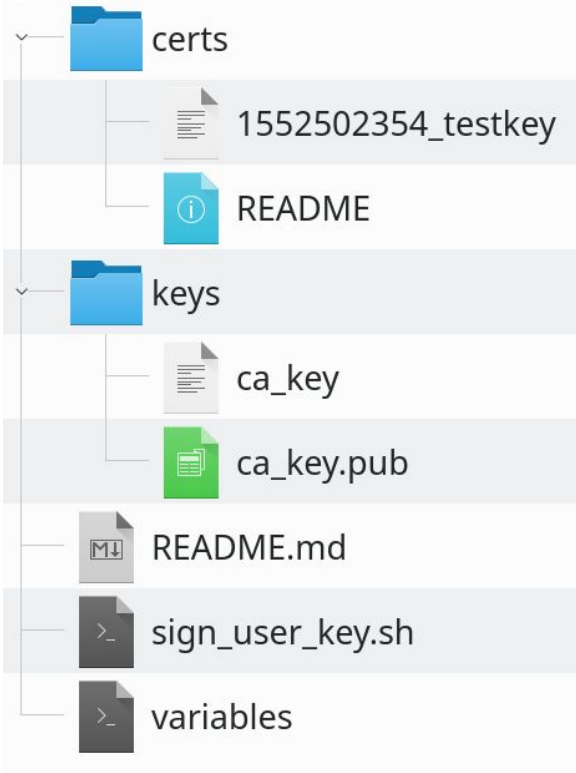
Demo

Implementation

- OpenSSH includes all necessary tools
- Multiple projects available
  - But usually large scale solutions

Implementation

- Our idea: small scale Implementation in git repository
- No additional infrastructure
- A single script
- All certificates in git



Demo

Credits for icons

- “Company”: geotatah via flaticon.com
- “Factory”: srip via flaticon.com
- “Employee”: Freepik via flaticon.com
- “Certificate”: Freepik via flaticon.com
- “Login”: Freepik via flaticon.com
- “Key”: Freepik via flaticon.com
- “Server”: Smashicons via flaticon.com

- Others: own work, Jiří Kraml, ZIGPOS GmbH

Any question?

Fork certificate repository at:

gitlab.com/zigpos/public-events/linux-days-prague-2019/ssh-certs