Zugang mit signierten SSH-Keys

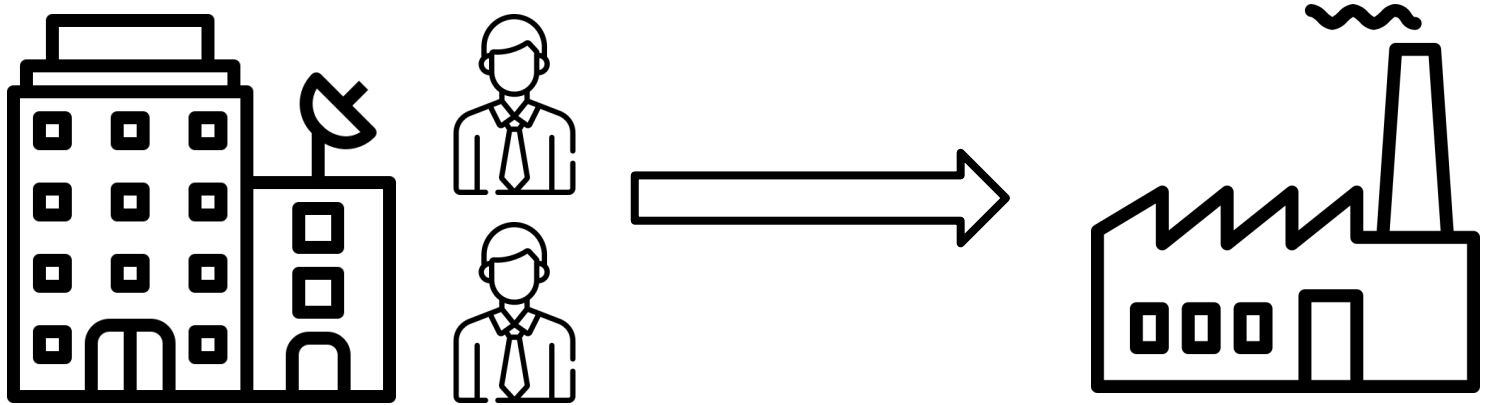
Jiří Kraml
Chemnitzer Linuxtage 2019

Ziel

- Mit SSH-Zertifikat auf VM anmelden

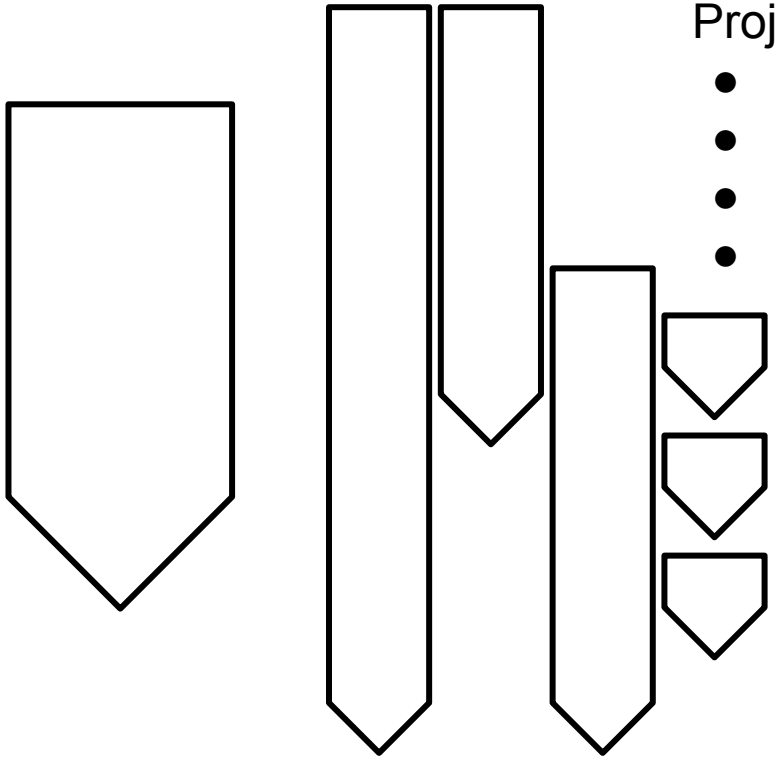
Ohne Login kein Service

- Lifecycle einer Appliance ≠ “Lifecycle” eines Projektmitglieds



Unterschiedliche Lifecycles

Appliance
- Auslieferung
- Update
- Entsorgung



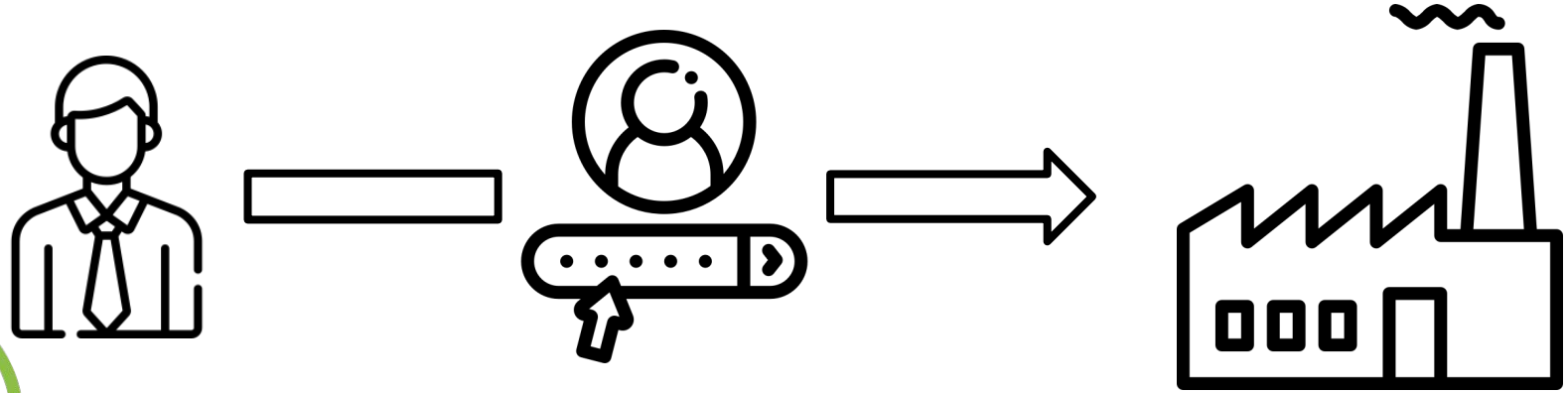
Projektmitglied
- Eintritt
- Andere Befugnisse
- Andere Aufgaben
- Austritt

Anmeldung per SSH

- Passwort
- Key Files
- Key Files + Zertifikat

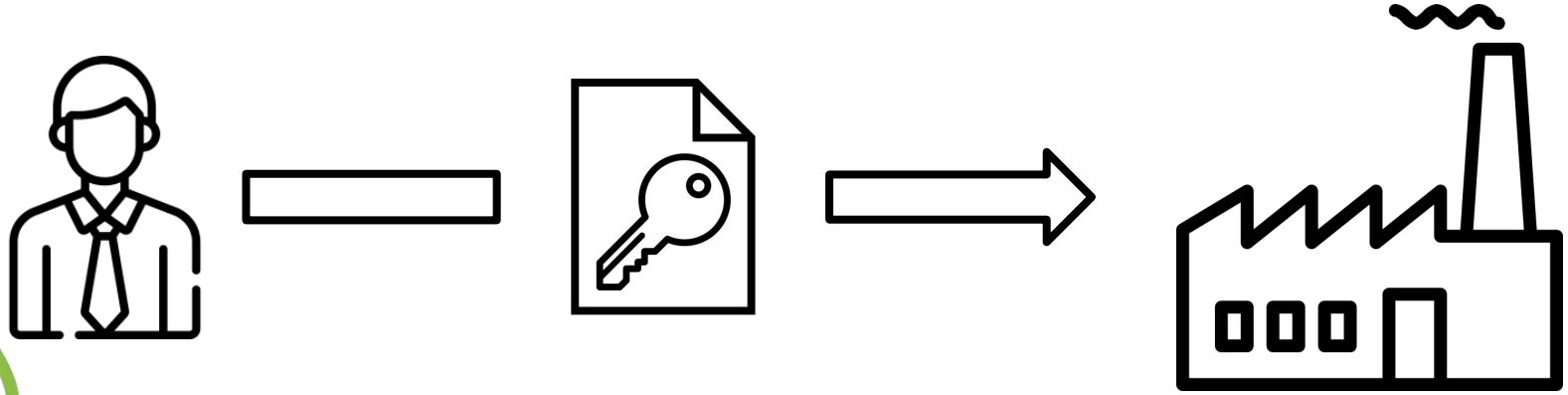
Passwörter weitergeben

- Meist nur ein Account
  - Also auch nur ein Passwort
  - Änderungen betreffen immer alle Nutzer



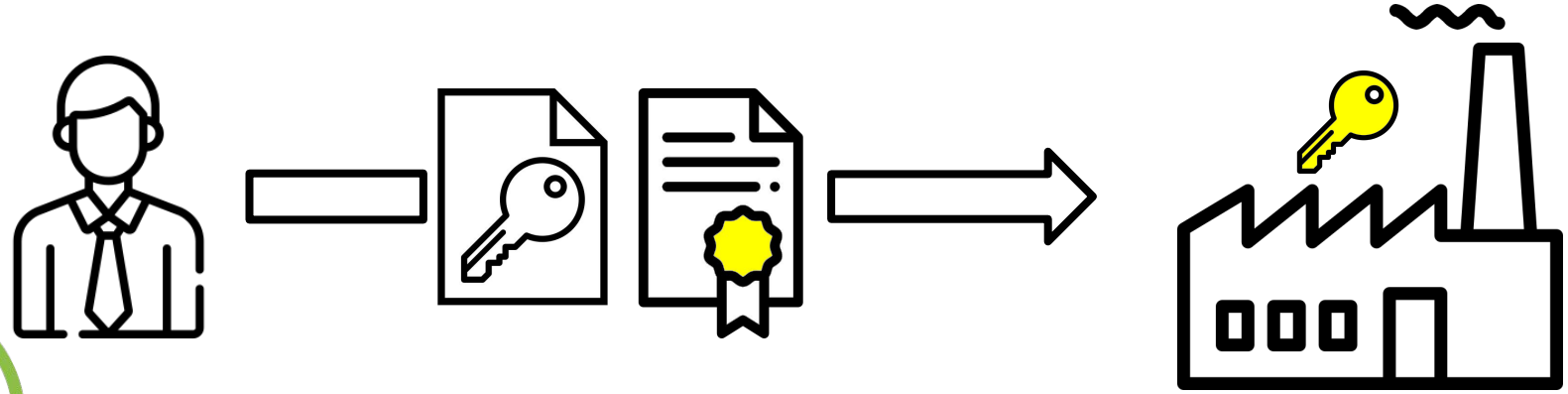
SSH Keys

- Beliebig viele pro Account
- Key-Pair ist ewig gültig
- Public Key muss Zielsystem bekannt sein



Signierte SSH Keys

- Gewohntes Key Pair, zusätzlich Zertifikat
  - Signature Public Key statt authorized_keys
- Beliebige Gültigkeit des Zertifikats
- OpenSSH Feature
- Systemzeit sicherheitsrelevant



Key Revocation Lists

- Zertifikat darf nicht weiterlaufen
- Widerrufung durch KRL
- KRL muss bekannt gegeben werden
- Public Keys können auch direkt widerrufen werden

Zertifikate im Lifecycle eines Projektmitglieds

Neues Mitglied	Neues Zertifikat
Mitglied bleibt	Zertifikat erneuern
Mitglied bekommt neue Aufgaben	Neues Zertifikat
Mitglied geht	Zertifikat auslaufen lassen oder auf Revocation List setzen

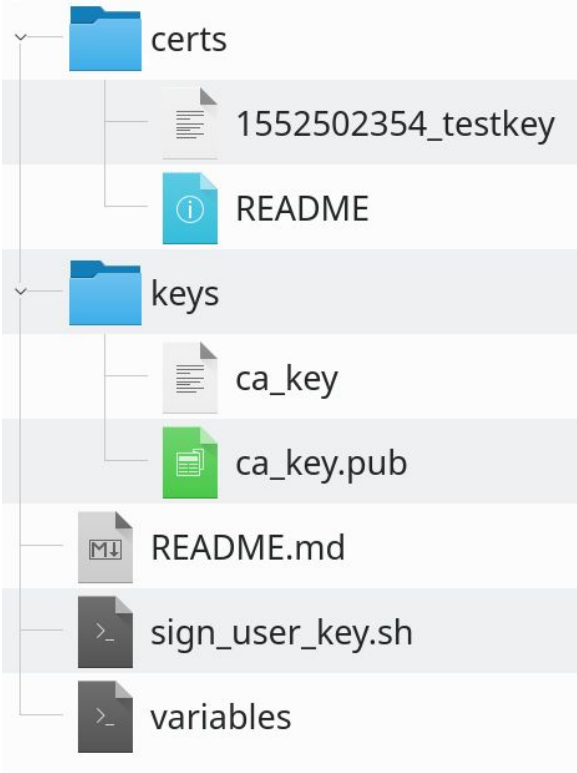
Demo

Umsetzung

- OpenSSH bringt alle Tools mit
- Mehrere Projekte bauen darauf auf
  - Meist jedoch sehr umfangreich

Umsetzung

- Unsere Idee: “kleine” Lösung in Git Repository
- Keine zusätzliche Infrastruktur
- Ein Skript
- Alle Zertifikate im Git



Bildnachweise

- “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

- Rest: selbstgemacht, Jiří Kraml, ZIGPOS GmbH

Fragen?

Präsentation und Begleitmaterial unter:
gitlab.com/zigpos/public-events/clt2019