Inhaltsverzeichnis

1 Überblick privacyIDEA

- Was sind Zwei Faktoren
- Was ist OTP
- Was ist privacyIDEA
- Dank an Yubico

2 Installation

```
add-apt-repository ppa:privacyidea/privacyidea
add-apt-repository ppa:yubico/stable
apt-get update
apt-get install privacyidea-apache2
apt-get install privacyideaadm
pi-manage.py admin add admin admin@localhost
```

(Hinweis auf privacyidea-dev)

Kontakt: cornelius.koelbel@netknights.it
+49 561 3166797
https://www.netknights.it

3 Konfiguration

3.1 Benutzer und Realms

- Anlegen des default realms
- → Man kann die Benutzer sehen
- Anlegen einer Datei /etc/privacyidea/users mittels

```
privacyidea-create-pwidresolver-user -u user1 -i 1001 -p user1 >> users
```

- Anlegen eines weiteren Realms aus der Datei /etc/privacyidea/users mit
- → Die Benutzer können sich mit dem Passwort aus der Datei anmelden. Das gilt auch für LDAP und SQL.

3.2 Administrative Nutzer

- Ein Realm „superuser“ wird angelegt entsprechend pi.cfg
- Die User können sich anmelden und haben administrative Rechte

3.3 Policies

- Betrachten wir erstmal heute nicht.

4 Token

4.1 Google Authenticator administrativ ausrollen

- Einen HOTP als Google Authenticator ausrollen und Benutzer zuweisen
- In Token Details anschauen und validieren

4.2 Google Authenticator für einen Benutzer ausrollen

- Einen HOTP als Google Authenticator ausrollen und Benutzer zuweisen
- In Token Details anschauen und validieren

Kontakt: cornelius.koelbel@netknights.it
+49 561 3166797
https://www.netknights.it

4.3 REST API

- /validate/check vorstellen, mit dem andere System mit privacyIDEA kommunizieren können

4.4 Yubikey ausrollen

- Einführung: Geht nur über Command line zu initialisieren

  ```
  privacyidea @secrets.txt token yubikey_mass_enroll
  ```

- Auch an der Kommandozeile können tokens angezeigt werden.

5 SSH

- Was gibt es alles? → apt-cache search privacyidea

  apt-get install privacyidea-pam

  dpkg -L privacyidea-pam

- Wir schauen in die Datei /etc/pam.d/common-auth-pi rein und setzen dort **nosslverify.**
- Nun können wir

  ssh piuser@localhost

  uns mit dem Passwort oder OTP anmelden.

Kontakt: cornelius.koelbel@netknights.it
+49 561 3166797
https://www.netknights.it