Enroll 2FA to thousands of users

Automating processes with privacyIDEA

FOSDEM 2018
Cornelius Kölbel
About Cornelius

- Cornelius Kölbel
- 2FA since 2005
  - Smartcards, Aladdin eToken, privacyIDEA since 2014
- Cornelius.koelbel@netknights.it
- @cornelinux
- @privacyidea
Challenges

• 2FA for services offered by city administration
Challenges

- End customers of electricity provider
Challenges

• 2FA for all university students!
Problems

- User will not come to admin desk
- User unknown
- User dislocated
- User not tech savvy
Problems

• User shoud not copy
Network structure

REST API, PAM, RADIUS, SAML, LDAP-Proxy, Win Cred Prov

Administration

REST API, Web UI, CLI, DB
privacyIDEA can manage different token types

- Key-fob Tokens
- OTP Cards
- SMS, Email, Smartphone
- Yubikey
- U2F
- eToken NG/OTP
- SSH Keys
- x.509-Certificates
- Meta-Tokens (Forward, RADIUS, 4eyes)
- ...

![Token types images]
Structure of privacyIDEA

- UI on Webserver
- REST API on Webserver
- Library level
- Database level

See: http://privacyidea.readthedocs.it
Possible automations

- Database (SQL)
- Library-Calls
- REST API-Calls
- Event Handler
• Python libs for **all** tasks.
• No need for REST API
  - No load on Webserver
• Tools for
  - expired users,
  - janitor for orphaned tokens
Example: automation via library

```python
for token_obj in tlist:
    try:
        if action == "disable":
            enable_token(serial=token_obj.token.serial, enable=False)
            print("Disabling token \{0\!s\}\".format(token_obj.token.serial))
        elif action == "delete":
            remove_token(serial=token_obj.token.serial)
            print("Deleting token \{0\!s\}\".format(token_obj.token.serial))
        elif action == "unassign":
            unassign_token(serial=token_obj.token.serial)
            print("Unassigning token \{0\!s\}\".format(token_obj.token.serial))
```
Call your API

- POST /validate/check
- POST /token/init
- GET /token/
- DELETE /token/OATH12344

See: http://privacyidea.readthedocs.it
Example: API automation

Generate tokens for users
Automation via Event Handler

- Trigger additional action
privacyIDEA HTTP Request

1. Pre policies (exceptions)
2. Request
3. Post policies (exceptions) → Response
4. Event Handler triggers additional action
ingredients

- Connected API calls
- Handler Module
  (notification, token, script, federation)
- Conditions
- Action with options
Example Event Handler

• If a paper token is generated by an administrator, the token will be disabled.

• It will be enabled if, the user authenticates with a registration code.

• The user gets notified, when his registration code is used.
Example: Event Handler

• To support external workflow, set arbitrary token attribute...
Example: Event Handler

• ...and run an external script!
Example: Event Handler

- (API call) /token/init
  - of registration code
- triggers script to
  - print welcome letter
Example: Event Handler

- /token/assign yubikey
- triggers token handler to set token attribute (needs shipping)
Graduate students: Token Janitor

- Token janitor can find and disable/delete unused tokens
Successful 2FA is a matter of smooth workflows.
• https://privacyidea.org
• https://github.com/privacyidea
  • @privacyidea
  • @cornelinux
• Cornelius.koelbel@netknights.it