Non-web federated access using QR-codes

Slávek Licehammer
slavek@ics.muni.cz

TNC19
18. 6. 2019

cesnet

MUNI

Authentication using QR code

- For non-web services

- Support for federated authentication (e.g. eduGAIN)

- Using standardized technology

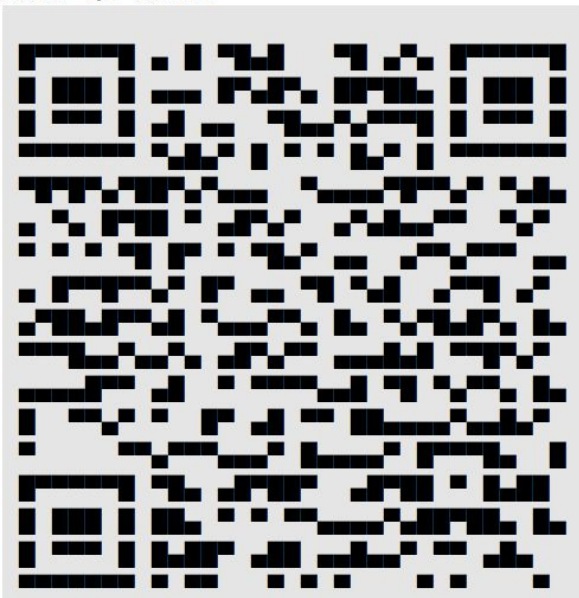- Minimal requirements on user / client side

- Easy to use

Demonstration
Access web server using SSH

```
ukko-3:~ michalp$ ssh root@cloud255-130.cerit-sc.cz
Scan QR code:
```



```
URL: https://login.elixir-czech.org/oidc/device?user_code=9RYJGX


Hit ENTER when you are done...▮
```

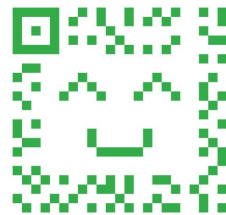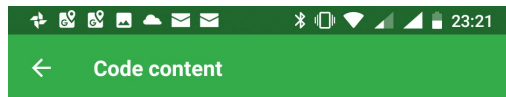Terminal Shell Edit View Window Help

michalp — ssh root@cloud255-130

lukko-3:~ michalp$ ssh root@cloud255-130.cerit-sc.cz
Scan QR code:

URL: https://login.elixir-czech.org/oidc/device?user_code=9RYJGX
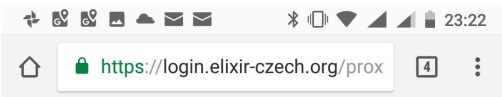
Hit ENTER when you are done...

Code content

URL is safe

https://login.elixir-czech.org/oidc/device?user_code=9RYJGX

Open

Share   Copy   Info

Screen 1

your previous selection

⭐ Masaryk University

or

G Sign in with Google
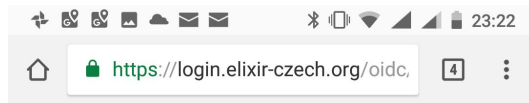
in Sign in with LinkedIn

iD Sign in with ORCID

or

your institutional account

🔍 Type the name of your institution

Aalborg University

Aalto University

Aarhus Basic Health Care College

Aarhus School of Marine and Technical Engineering

Screen 2

Approval Required for *ELIXIR Cloud Demo*

🌐 **Caution:**
This client was dynamically registered .
It has been approved {0} times previously.
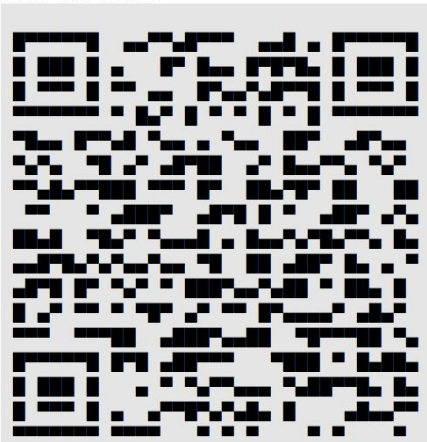
Access to:

- 👤 Log in using your identity

Do you authorize "ELIXIR Cloud Demo"?

Authorize   Deny

```
[ukko-3:~ michalp$ ssh root@cloud255-130.cerit-sc.cz
Scan QR code:
```



```
URL: https://login.elixir-czech.org/oidc/device?user_code=NOTYCM


Hit ENTER when you are done...
Linux cloud255-130 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) x86_64


   ___ ___ ___ _ _____    ___  ___
  / __| __| _ \| |_   _|__/ __|/ __|'s cloud image with *cloud-init*
 | (__| _||   /| | | | ||___\__ \ (__    http://www.cerit-sc.cz/
  \___|___|_|_\|_| |_|   |___/\___|


Last login: Fri Jun  1 15:26:43 2018 from 147.251.13.8
root@cloud255-130:~#
```

Technological background

- Out of band authentication

- OpenID Connect (OIDC)

  - Standardized OAuth2 Device flow

- Pluggable Authentication Module (PAM)

  - Can be used by any application supporting PAM

  - PAM module with OAuth2 Device flow support

- Easy to use for user

  - Retype URL to browser

  - Scan QR code to device with browser

Future steps and ideas

- OIDC agent (ssh-agent analogy)

  - Proof of concept implementation exists

  - Using modified Dropbear SSH server

  - OIDC agent have to be installed on client side

- Using on any device which is able to display QR code

  - Shared printers, access to rooms, IOT

- Mobile app instead of federated sing in in web browser

  - Single sign-on

  - Easier (faster) to use

Thank you for your attention

Source code for PAM module:
https://github.com/ICS-MU/pam_oauth2_device

Slávek Licehammer
slavek@ics.muni.cz

TNC19
18. 6. 2019