

Autentizace QR kódem

Slávek Licehammer

slavek@ics.muni.cz

Seminář o bezpečnosti sítí a služeb

31. 1. 2019



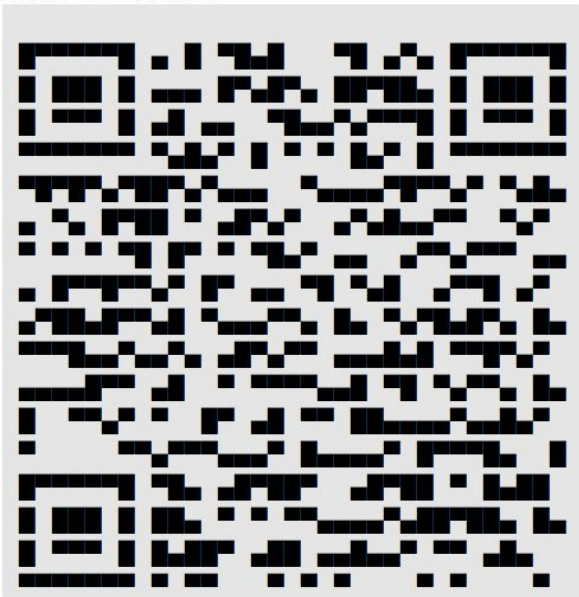
Použití autentizace QR kódem

- Pro newebové služby
 - Podpora federované autentizace (např. s využitím eduID.cz)
 - Využití standardních technologií
 - Minimální nároky na uživatele
-
- Ukázka na přístupu na stroj pomocí SSH

micHALP — ssh root@cloud255-130.cerit-sc.cz -

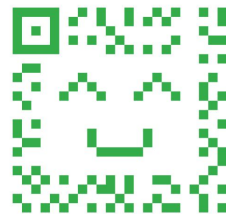
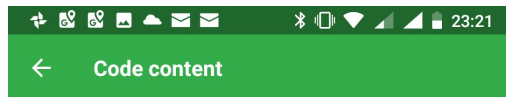
ukko-3:~ micHALP\$ ssh root@cloud255-130.cerit-sc.cz

Scan QR code:



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

Hit ENTER when you are done... █



URL is safe

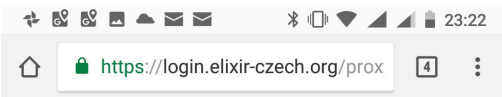
https://login.elixir-czech.org/oidc/device?user_code=9RYJGX



Share

Copy

Info



your previous selection

★ Masaryk University

or


 Sign in with Google

 Sign in with LinkedIn

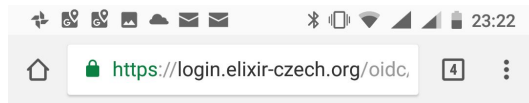
 Sign in with ORCID

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




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

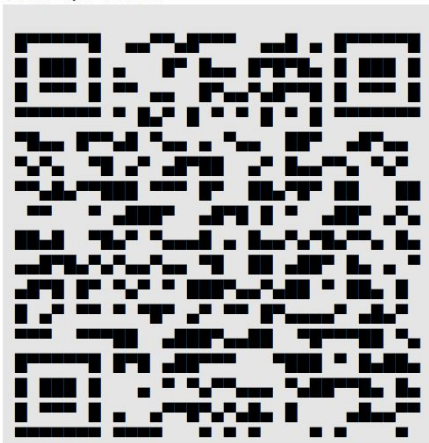
Do you authorize "ELIXIR Cloud
Demo"?

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/
  \ _ | _ | _ \ | | | | _ \ / _ |

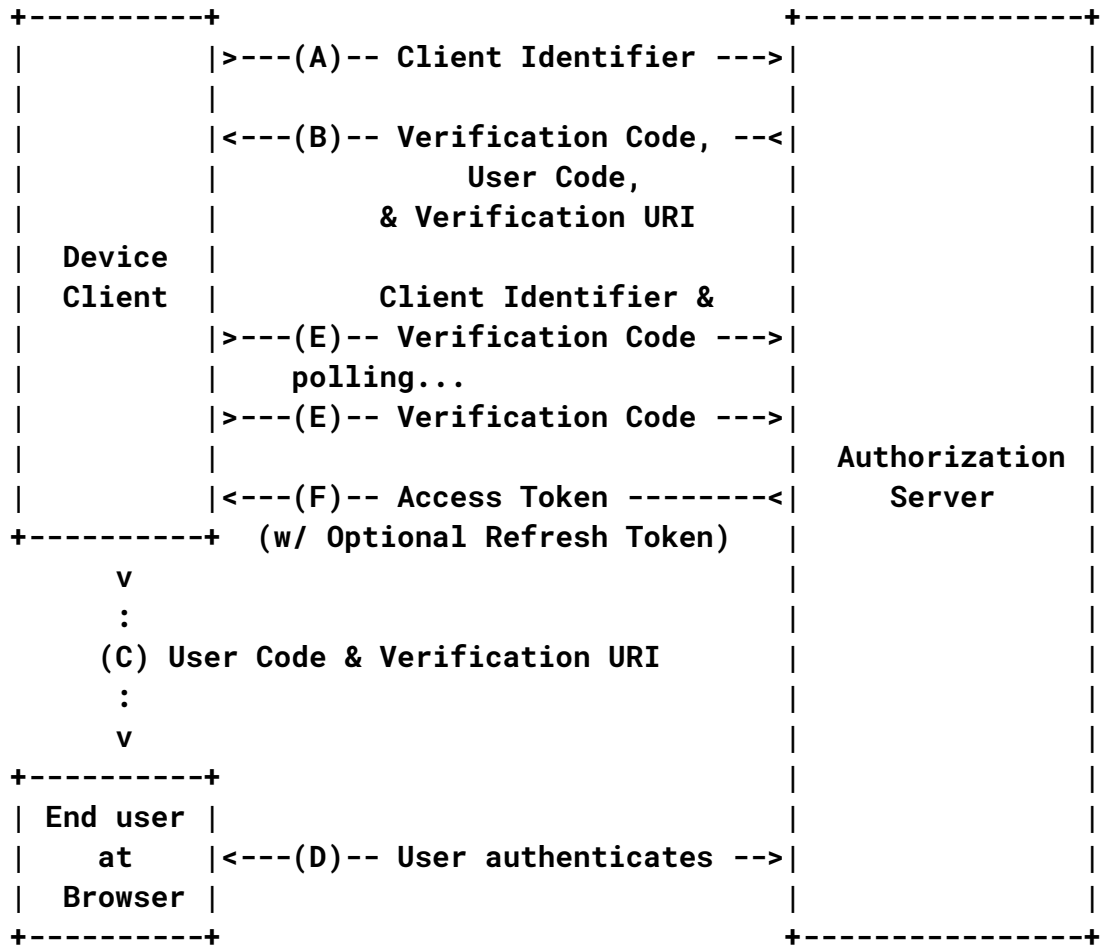
```

Last login: Fri Jun 1 15:26:43 2018 from 147.251.13.8

root@cloud255-130:~# █

Použité koncepty a technologie

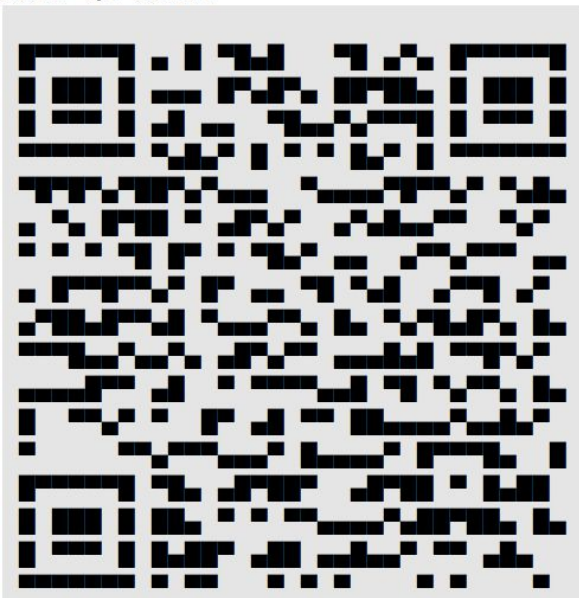
- Out of band autentizace
- OpenID Connect (OIDC)
 - Standardizované OAuth2 Device flow
- Pluggable Authentication Module (PAM)
 - PAM modul s podporou OAuth2 Device flow
 - Lze použít pro jakoukoliv službu podporující PAM
- Jednoduché pro uživatele
 - Stačí vyfotit QR obsahující URL
 - Alternativně lze URL přepsat ručně
- Single sign-on



micHALP — ssh root@cloud255-130.cerit-sc.cz -

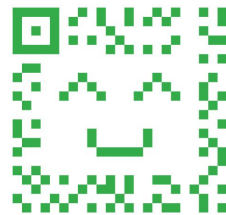
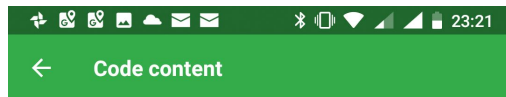
ukko-3:~ micHALP\$ ssh root@cloud255-130.cerit-sc.cz

Scan QR code:



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

Hit ENTER when you are done... █



URL is safe

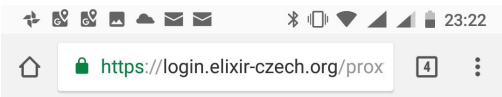
https://login.elixir-czech.org/oidc/device?user_code=9RYJGX

Open

Share

Copy

Info



your previous selection

★ Masaryk University

or


 Sign in with Google

 Sign in with LinkedIn

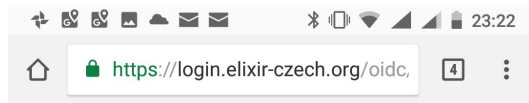
 Sign in with ORCID

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




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

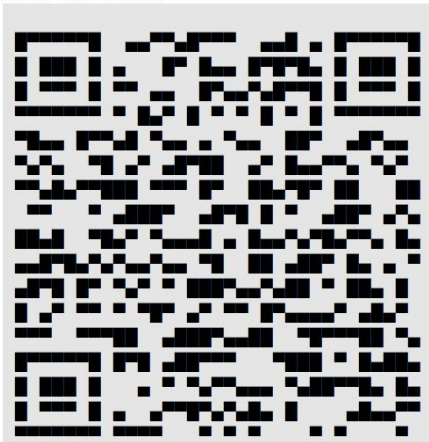
Do you authorize "ELIXIR Cloud
Demo"?

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:~# █

Možná využití a rozšíření

- **OIDC agent (obdoba ssh-agent)**
 - Proof of concept implementace
 - Modifikace Dropbear SSH serveru
 - Nutnost mít OIDC agent nainstalovaný na klientské straně
- **Použití na libovolném zařízení schopné zobrazit QR kód**
 - Sdílené tiskárny, náhrada karet na zabezpečení místností, IOT zařízení
- **Aplikace v mobilu jako náhrada federovaného přihlášení**
 - Single sign-on
 - Jednodušší na použití

Děkuji za pozornost

Zdrojový kód PAM modulu:

https://github.com/ICS-MU/pam_oauth2_device

Slávek Licehammer

slavek@ics.muni.cz

Seminář o bezpečnosti sítí a služeb

31. 1. 2019

