# ELIXIR AAI Advanced Features

*Michal Procházka, ELIXIR-CZ*

*DI4R Lisbon*
*10 Oct 2018*

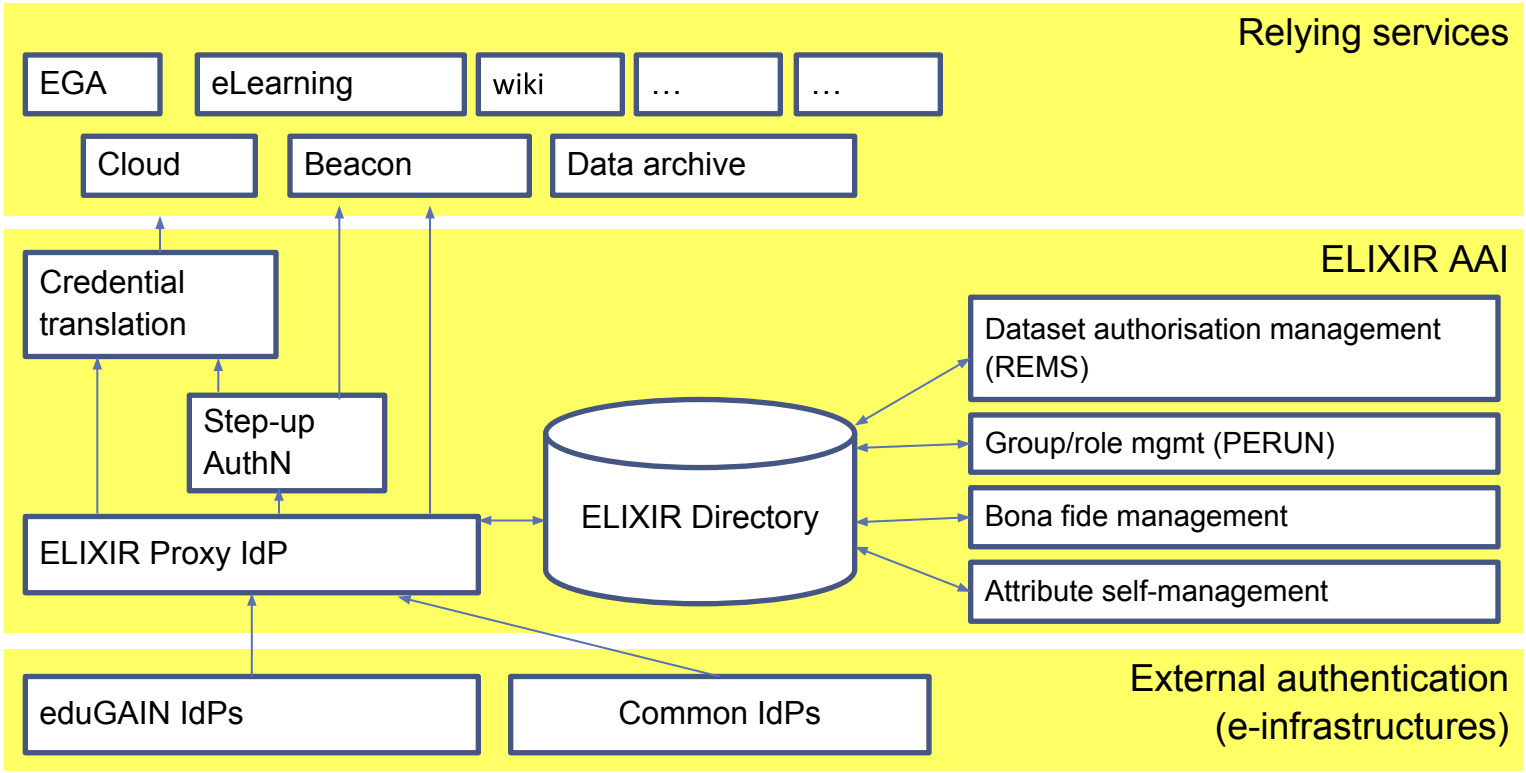
*www.elixir-europe.org*

# ELIXIR AAI (authentication and authorisation infrastructure)

- ELIXIR Compute platform's service portfolio for authenticating researchers and helping other services to decide their permissions
- Being implemented as an ELIXIR infrastructure service from 2019
- Will underpin Life Science AAI with other RIs

- Follows the AARC Blueprint architecture

# ELIXIR AAI design



# Selected advanced features

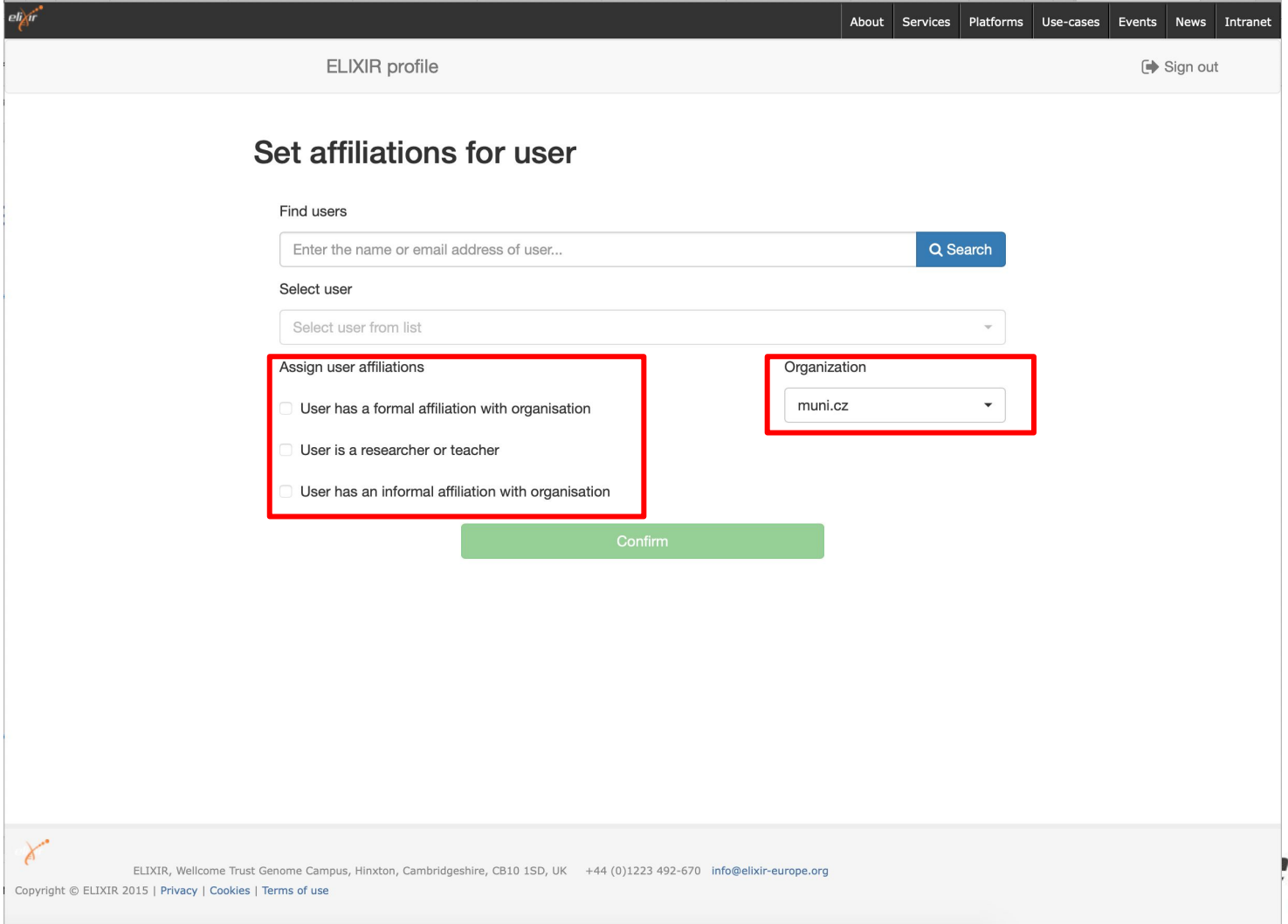
- Management of user's affiliation
- Access Control Enforcement
- Permissions API
- Accessing non-web resources
- Advanced service integration

# Management of user's affiliation

- Services need to know affiliation of the user
  - Researcher? Student? Formally affiliated with the institution?
  - For authorization
- Not all institutions release affiliation via federated login
- Social providers cannot release user's affiliation

- How to get valid user affiliation in a distributed environment?

- Selected trusted users from institutions who can assign user affiliation
  - Authorization is based on scopes (domains)


About
Services
Platforms
Use-cases
Events
News
Intranet
ELIXIR profile
Sign out
Set affiliations for user
Find users
Enter the name or email address of user...
Search
Select user
Select user from list
Assign user affiliations
User has a formal affiliation with organisation
User is a researcher or teacher
User has an informal affiliation with organisation
Organization
muni.cz
Confirm
ELIXIR, Wellcome Trust Genome Campus, Hinxton, Cambridgeshire, CB10 1SD, UK +44 (0)1223 492-670 info@elixir-europe.org
Copyright © ELIXIR 2015 | Privacy | Cookies | Terms of use

# Access Control Enforcement

- Some services would like to do the authorization, but they don’t have capabilities
  - Proprietary software
  - Old software
  - Too expensive to modify the software
- Authorization is enforce on the Proxy
- Authorization is based on groups
  - Users who are member of the group has a right to access the service
- Users without permissions can be redirected to the registration page
- Service can enable/disable access control enforcement

# Access forbidden

You don't meet the prerequisites for accessing the service: de.NBI Cloud Portal
For more information about this service please visit this https://cloud.denbi.de

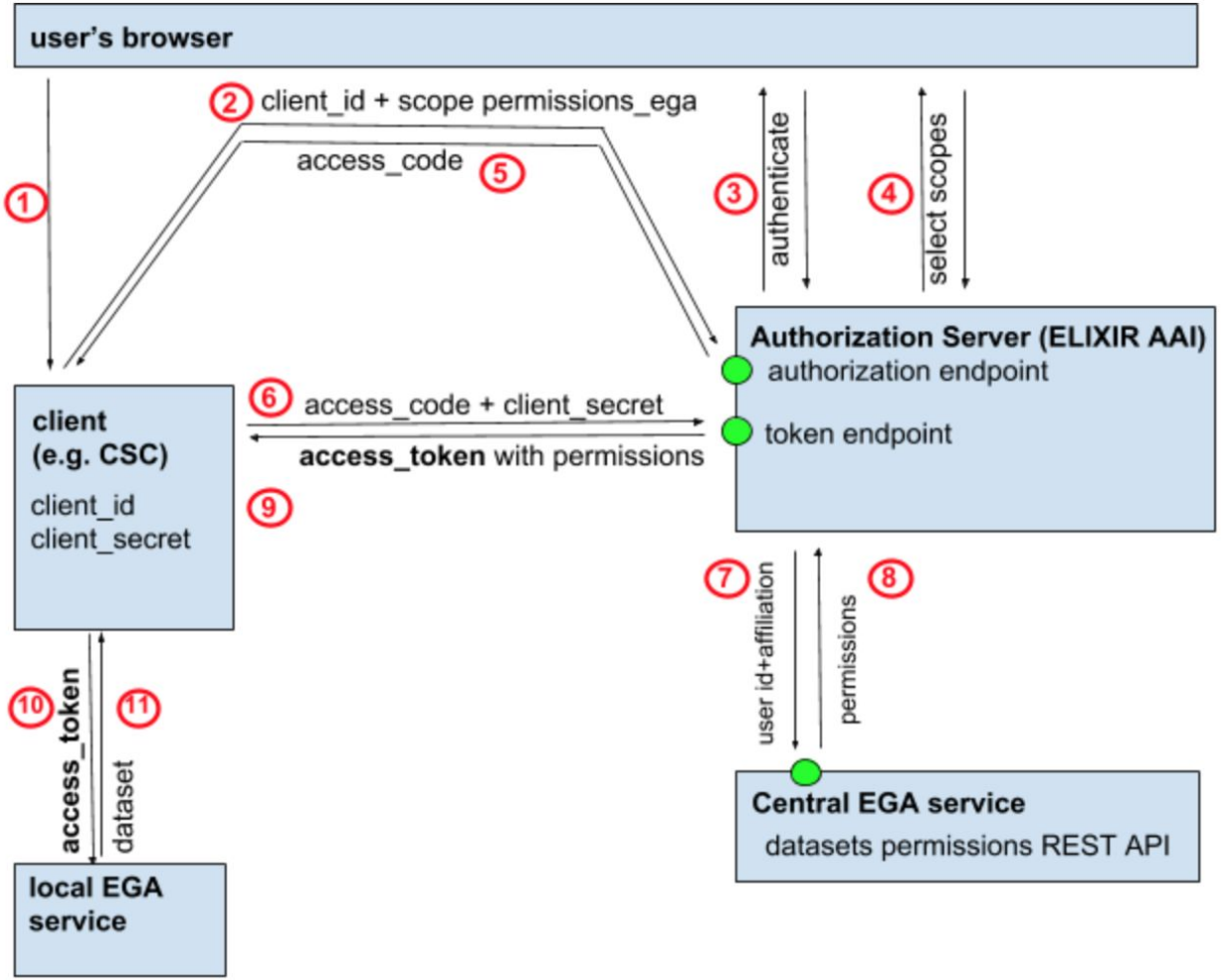
If you think you should have an access contact service operator at cloud@denbi.de

ELIXIR, Wellcome Trust Genome Campus, Hinxton, Cambridgeshire, CB10 1SD, UK +44 (0)1223 492-670 info@elixir-europe.org

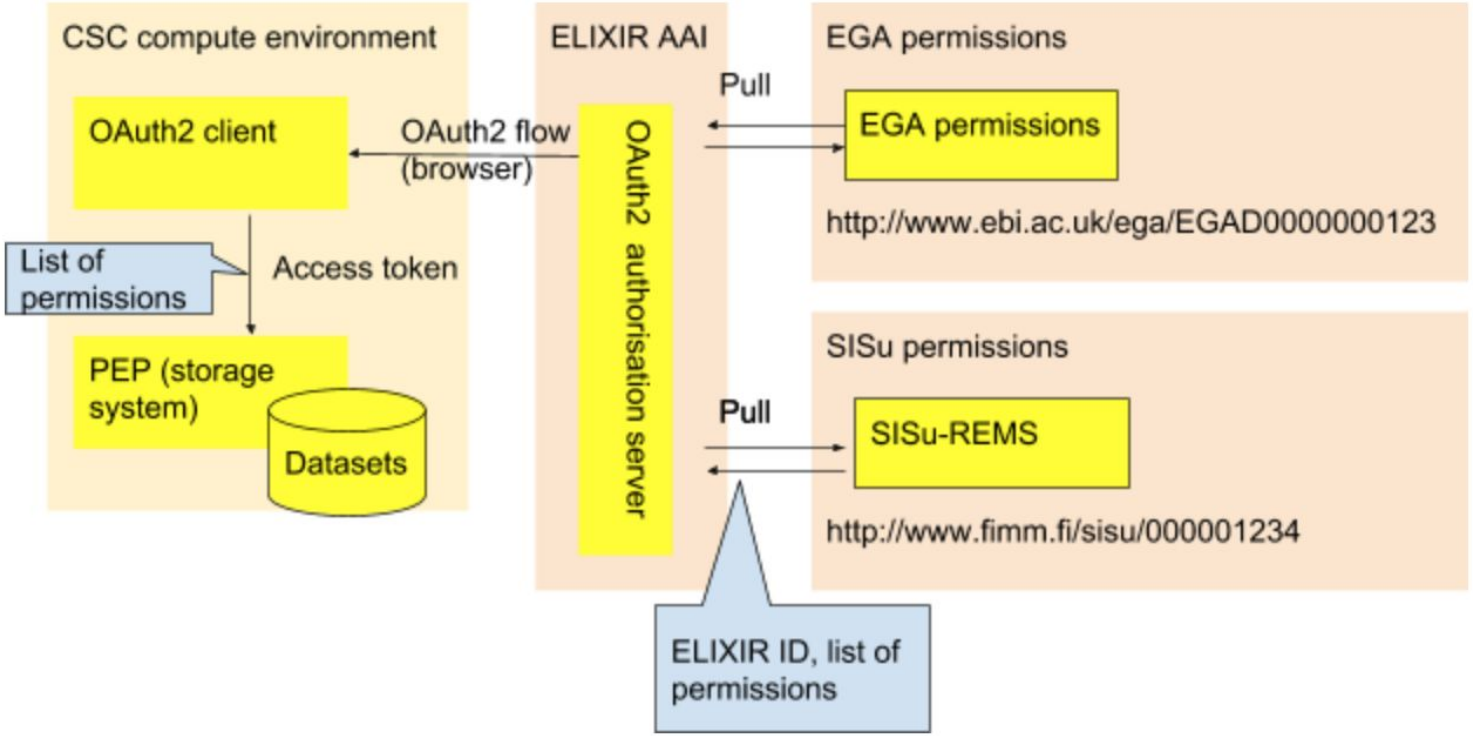
Copyright © ELIXIR 2018 | Privacy | Cookies | Terms of use

# Permissions API

- Managing access to the datasets (sensitive data)
  - Proper authorization is needed
- Authorization data are stored outside the ELIXIR AAI
  - Can be even stored in multiple places
- Leveraging ELIXIR AAI Single Sign-On
- ELIXIR AAI delivers authorization data in a standard way to the services


user's browser
1
2 client_id + scope permissions_ega
access_code 5
3 authenticate
4 select scopes
Authorization Server (ELIXIR AAI)
authorization endpoint
token endpoint
client
(e.g. CSC)
client_id
client_secret
6 access_code + client_secret
access_token with permissions
9
7 user id+affiliation
8 permissions
10 access_token
11 dataset
local EGA
service
Central EGA service
datasets permissions REST API

# Permissions API



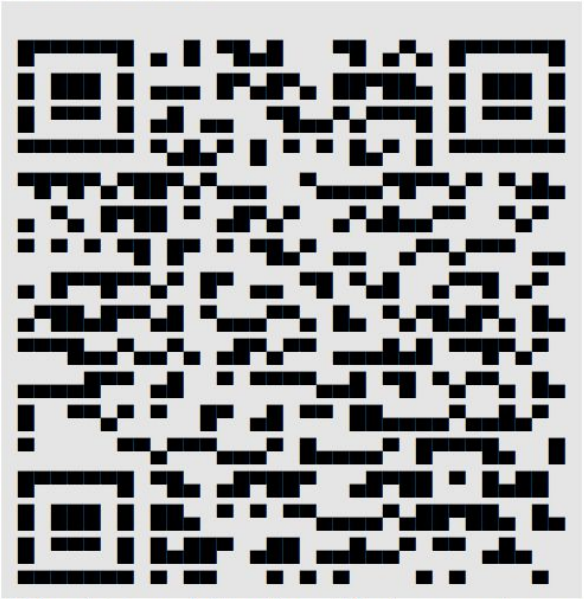
# Accessing non-web resources

- How to access non-web resources using federated identity?
  - SSH or VNC on a cloud machine
  - Mounting data storages
  - Access instruments with attached PC (limited display capabilities)

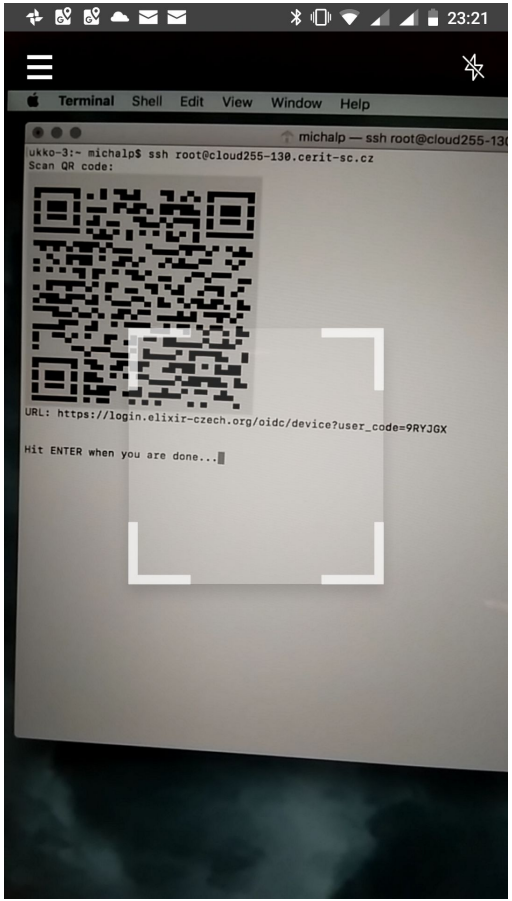
- Experimental solution in ELIXIR AAI
  - Standardized OAuth2 device code flow
  - Out of band authentication
  - Pluggable Authentication Module (PAM)
    - Can be used by any application supporting PAM
  - PAM module with OAuth2 device flow support

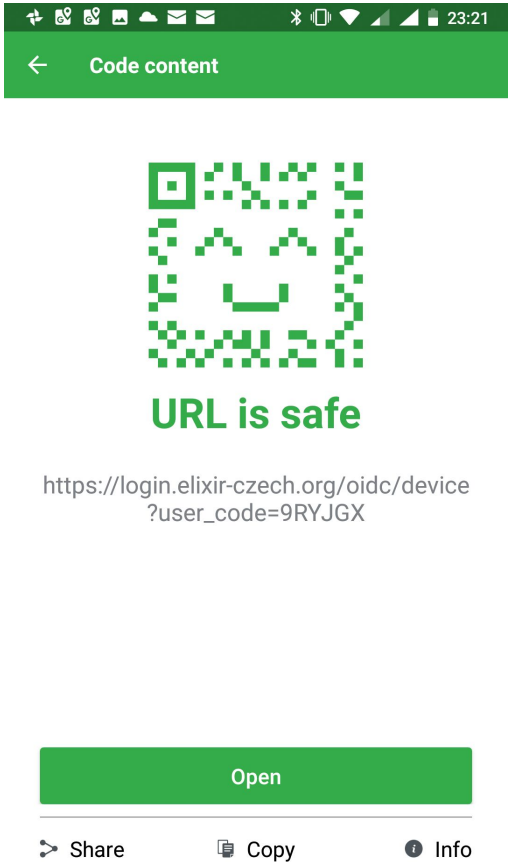
michalp — ssh root@cloud255-130.cerit-sc.cz -

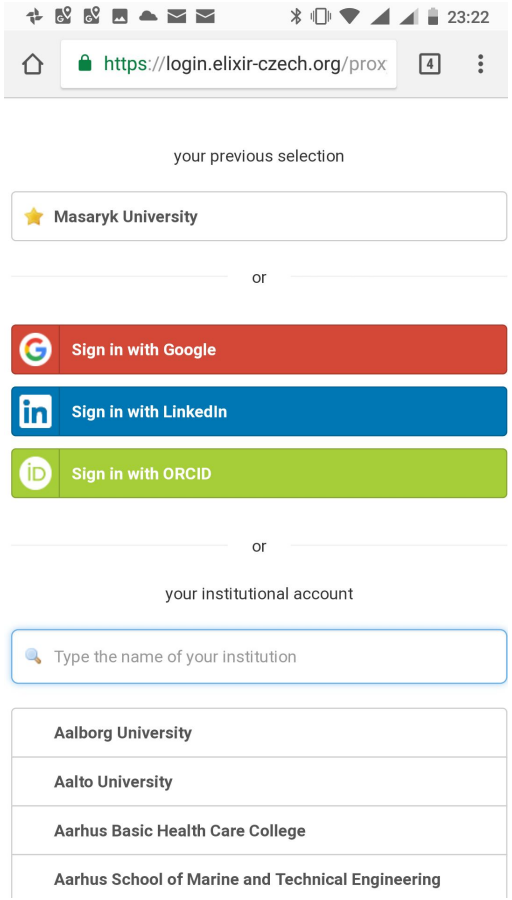
```
ukko-3:~ michalp$ ssh root@cloud255-130.cerit-sc.cz
Scan QR code:
```

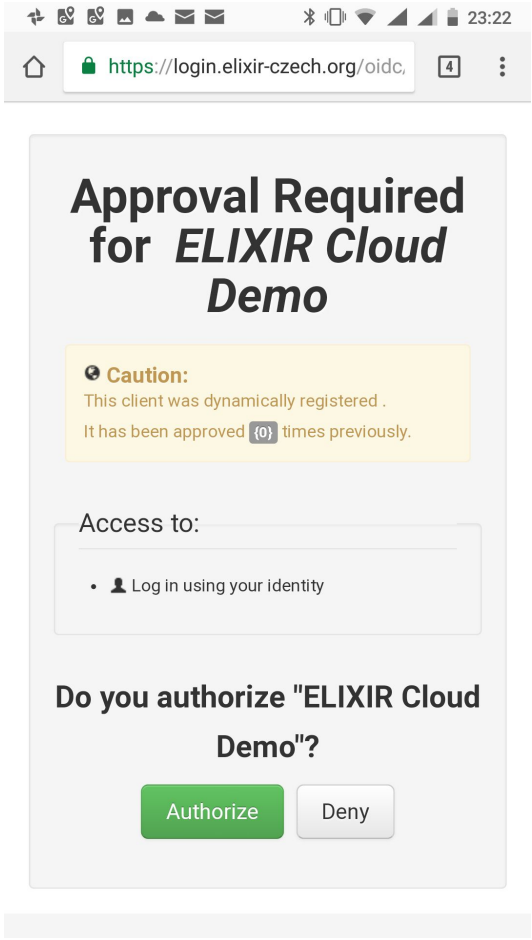


```
URL: https://login.elixir-czech.org/oidc/device?user_code=9RYJGX

Hit ENTER when you are done...
```

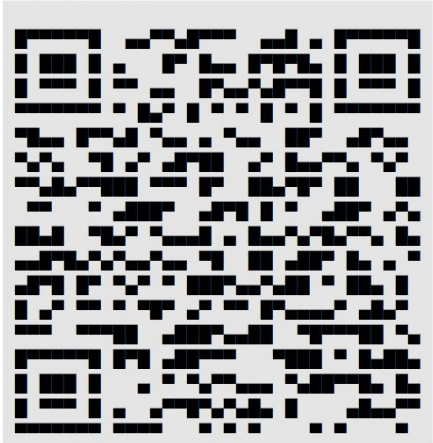

23:21
Terminal Shell Edit View Window Help
michalp — ssh root@cloud255-130
ukko-3:~ michalp$ ssh root@cloud255-130.cerit-sc.cz
Scan QR code:
URL: https://login.elixir-czech.org/oidc/device?user_code=9RYJGX
Hit ENTER when you are done...


23:21
Code content
URL is safe
https://login.elixir-czech.org/oidc/device
?user_code=9RYJGX
Open
Share
Copy
Info


23:22
https://login.elixir-czech.org/prox
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


23:22
https://login.elixir-czech.org/oidc,
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

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

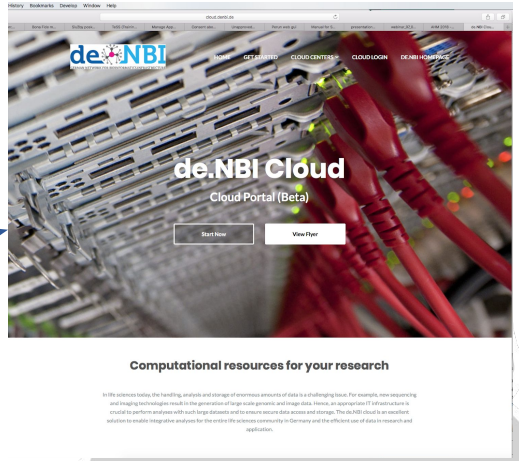


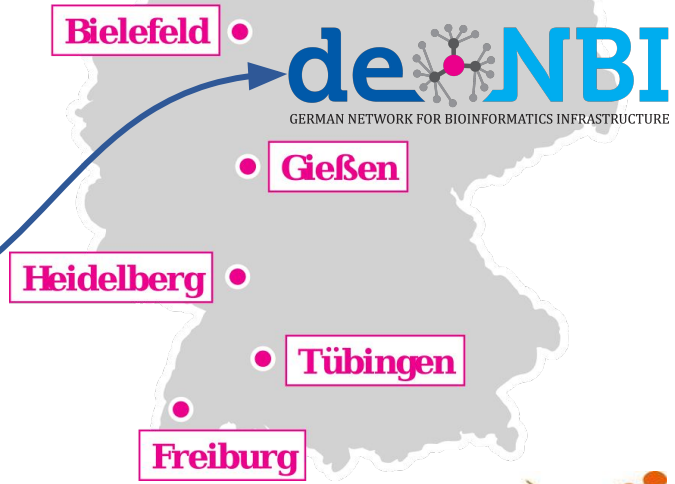
```
URL: https://login.elixir-czech.org/oidc/device?user_code=NOTYCM


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:~#
```

# Advanced service integration

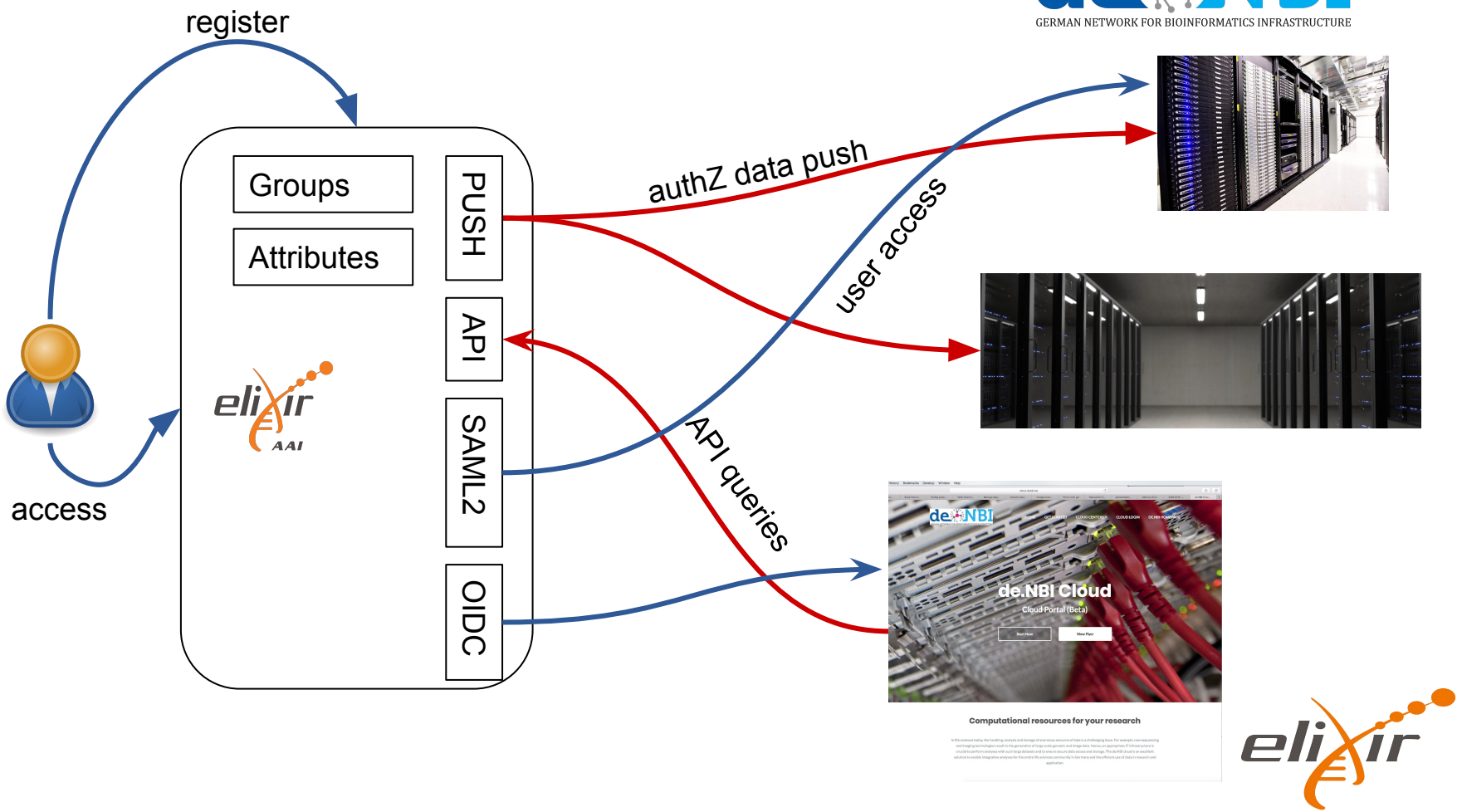
- User accounts created in advance
- Deprovisioning of the user accounts
- Groups managed via the service itself
- Additional data (e.g. project name)
- Custom user registration

elixir LOG-IN




elixir


register
Groups
Attributes
PUSH
API
SAML2
OIDC
elixir AAI
access
authZ data push
user access
API queries
de.NBI Cloud
Cloud Portal (Beta)
Computational resources for your research

# More information on ELIXIR AAI

https://www.elixir-europe.org/services/compute/aai

Paper

- Linden et al: Common ELIXIR service for Researcher authentication and authorisation. F1000 Research, 2018

Software

- Perun Keystone Adapter
  - https://github.com/deNBI/perunKeystoneAdapter
- Python Social API
  - https://github.com/python-social-auth/social-core

# Thank you for your attention

michalp@ics.muni.cz

*www.elixir-europe.org*

*@ELIXIREurope*

*/company/elixir-europe*